Pro Patria ad Deum

UNIVERSIDAD DE LA FRATERNIDAD DE AGRUPACIONES

SANTO TOMÁS DE AQUINO

Facultad de Ciencias Jurídicas y Sociales

Carrera: Licenciatura en Seguridad Ciudadana

Título: Estafas virtuales en el Departamento San Jerónimo, Provincia de Santa Fe, en el segundo semestre del año 2023.

Autor: Natalia Verónica Trobbiani

Correo: nati_ailu82@hotmail.com

Tutores: MG.Paula Ariadna Jessurum y Lic. Rocio Dominguez

Año de Presentación: 2025

AGRADECIMIENTOS

A NUESTRO SEÑOR DIOS Y LA VIRGEN MADRE QUE ME DIERON LA POSIBILIDAD DE LLEVAR ADELANTE ESTE NUEVO DESAFIO

A MI FAMILIA POR SU APOYO INCODICIONAL Y ACOMPAÑAMIENTO

A MI MADRE QUE SIEMPRE ACOMPAÑO CON SUS BENDICIONES

A TODOS LOS PROFESORES QUE ESTUVIERON EN ESTA CURSADA POR LA DEDICACION Y RESPETO

MUCHAS GRACIAS

ÍNDICE

TRABAJO FINAL

TEMA: Estafas virtuales en el Departamento San Jerónimo, Provincia de Santa Fe, en el segundo semestre del año 2023.

1. INTRODUCCIÓN

La ciberdelincuencia es una de las formas de delincuencia más importantes y activas del mundo. Después de todo, Internet está disponible y es visible para todos, y eso, por supuesto, implica riesgos. Cometer un delito a través de una computadora u otro dispositivo que esté conectado a Internet es peligroso porque la identidad del perpetrador es difícil de averiguar.

En realidad, no hubo ningún delito cibernético real hasta la década de 1980. Donde una persona hackeó la computadora de otra persona para encontrar, copiar o manipular datos e información personal. La primera persona en ser declarada culpable de un delito cibernético fue Ian Murphy, también conocido como Capitán Zap, y eso sucedió en el año 1981. Había pirateado la compañía telefónica estadounidense para manipular su reloj interno, de modo que los usuarios aún pudieran realizar llamadas gratis en horas pico.

Las primeras conductas indebidas o ilícitas relacionadas con computadoras comenzaron a verse reflejados durante la década del 70, a partir de algunos casos resonantes retratados por los periódicos de época. Los primeros delitos informáticos eran de tipo económico, entre los que se destacaban el espionaje informático, la “piratería” de software, el sabotaje a bases de datos digitalizados y la extorsión. En relación con el espionaje, estos se llevaban a cabo mediante la extracción de discos rígidos de las computadoras, el robo de diskettes o copia directa de la información de los dispositivos, tanto, así como la absorción de emisiones electromagnéticas que irradia toda computadora para la captación de datos. El espionaje era comercial o industrial, como suele denominarse, siendo sus principales objetivos los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco del espionaje industrial. Los casos de sabotaje y extorsión informática eran los delitos

que más preocupaban organizaciones ante la alta concentración de datos almacenados en formato digital. En cuanto a los fraudes de tipo financiero, a fines de esa década y principios del 80, hubo casos de alteración de archivos de las bases de datos de las empresas y los balances de los bancos para la manipulación de facturas de pagos de salarios. Casos típicos se realizaban mediante la instalación de dispositivos lectores, en las puertas de entradas de los cajeros automáticos, y teclados falsos, en los mismos, para la copia de los datos de las tarjetas de débito a través de la vulneración de las bandas magnéticas. Esto motivó, por parte de las empresas emisoras, la adopción de chips, en los plásticos, como medida de seguridad. Cabe mencionar justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.

Los piratas informáticos, sin embargo, procedieron de diferentes maneras a lo largo del tiempo. Aunque las empresas telefónicas fueron el primer objetivo, los bancos, las tiendas web e incluso los particulares siguieron rápidamente su ejemplo. Hoy en día, la banca en línea es muy popular y eso también conlleva un gran riesgo. Por ejemplo, los piratas informáticos pueden copiar códigos y nombres de inicio de sesión o recuperar contraseñas de tarjetas de crédito y cuentas bancarias. El resultado es que uno puede simplemente vaciar cuentas o hacer compras en línea con la cuenta de otra persona.

En Argentina el primer caso de ciberdelito se dio en el año 1999, este ha ido en aumento en las últimas décadas, con casos fraude, robo de información, suplantación de identidad y otros delitos cibernéticos. Las autoridades argentinas han implementado leyes y medidas para combatir este tipo de delitos, como la Ley de Delitos Informáticos. Sin embargo, la lucha contra el ciberdeltios sigue siendo una lucha en el país, con un aumento constante de la actividad delictiva en línea.

En nuestro país todos estos delitos por fraudes o estafas electrónicos están plasmados en el artículo 172 “será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, créditos, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño” y 173 inc. 15 y 16 del Código Penal y este sancionan la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. La ley 26388 (delitos informáticos), promulgada en junio del 2008, incorpora los delitos cometidos por medios informáticos, uno de los principales delitos informáticos que se cometen en argentina es el Phishing el inc. 16 del art 173 del C.P.A “el que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento o transmisión de datos”. Lo satisfactorio de la ley de Delitos Informáticos (Ley 26388) es que el legislador adopta una técnica legislativa amplia, de manera que cualquier técnica informática sea comprendida en este delito.

En el año 2020 la Argentina encabezo el ranking de cibercrimen en Americana la Latina, con un total de alrededor de un 40 % de los delitos en el país, según el informe presentado por la Unidad Fiscal Especializada en Ciberdelincuencia. Durante la pandemia, el cibercrimen en Argentina aumento elocuentemente en virtud a que muchas personas se vieron impulsadas al uso de la tecnología, sin tener en cuenta el riesgo de inseguridad. Se registraron más estafas online, phishing, robo de información personal y fraudes financieros. Esto afecto a individuos, empresas organizaciones, generando pérdidas económicas y problemas de seguridad informática.

Los delitos por estafas virtuales denunciados en las diferentes comisarías jurisdiccionales correspondientes al Departamento San jerónimo de la provincia de Santa Fe, y elevadas a la fiscalía Regional con asiento en la ciudad de Coronda dependiente del Ministerio Publico de la Acusación Santa Fe, en el segundo semestre del año 2023, pertenecen en algunas casos, a transferencias o débitos automáticos a otras cuentas engañosas (phishing), otras por medio de páginas web con perfiles falsos, redes sociales, direcciones de correos electrónico con virus

(pharming), en su mayoría llamadas telefónicas (vishing) SMS, mensajes de WhatsApp (smishing). Efectuada una compulsa sobre los registros estadísticos que se llevan en esta jefatura departamental (oficinas de división judicial-División informaciones), las denuncias realizadas por estafas virtuales, se han incrementado entre los meses de Julio y diciembre del año 2023, en un porcentaje del 100% respecto primer semestre del año 2023, donde se registró un total de 66 denuncias, por lo que contabilizando que durante el segundo semestre del año 2023, se registraron un total de 133 denuncias por ciberdelitos , un el 30,075 % fueron denunciados en la Ciudad de Coronda cabecera departamental, con un total de 40 casos registrados, en otra ciudad importante, es la Ciudad de Gálvez donde se registró un 24,81 de casos con la cantidad de 33 denuncias, en tanto en la localidades como Barrancas fue de un 11,27 % con 15 casos, Maciel un 8,27 % con 11 casos, San Genaro con un 19,54 % con 26 casos y Centeno con un 6,01% con 8 casos. La presente investigación tiene como objetivo final, proporcionar información que sea de utilidad a toda la población, para así generar en la misma conciencia, un conocimiento y habilidades propias para poder identificar y evitar caer e estafas virtuales. Aportar para extender los datos sobre este tipo de delito en este departamento y franjas afectadas para estudiar posibles nuevas variantes.

1.1 Problema:

¿Cuáles fueron las características y la modalidad adoptada de las estafas virtuales en el Departamento San Jerónimo, en el segundo semestre del año 2023?

1.2. OBJETIVOS

1.2 Objetivo general.

Analizar las características de los casos de estafas virtuales ocurridas, en el departamento San Jerónimo Provincia de Santa Fe, en el segundo semestre del año 2023.

1.3 Objetivos específicos.

-Identificar a los delincuentes, determinar quiénes están detrás de las estafas y seguir algún rastro digital para dar con su identidad.

-Determinar los modus operandi de las estafas virtuales.

-Identificar los diferentes tipos de estafas virtuales.

-Determinar la franja horaria, días de la semana y mes en que producen estos fraudes.

-Determinar las edades y sexo de las víctimas de las estafas.

_Determinar las principales causas de este delito.

-Determinar la zona de las localidades que exhiben mayor cantidad de denuncias.

-Identificar los canales utilizados por los ciberdelincuentes para cometer el delito estafa virtual o electrónica.

-Determinar las motivaciones con los que el delincuente inicia el contacto con su posible víctima.

-Identificar los valores o montos sustraídos a las víctimas de estafas.

2. MÉTODO

La presente investigación será de tipo básico, con un diseño no experimental, de alcance transversal y descriptivo-respectivo. Se evaluarán las variables luego de consumado el hecho, sin manipular la variable independiente. De esta manera, mediremos lo que existe y lo que motiva las variables dependientes.

Estudiaremos a nivel cuantitativo el total de casos de estafas virtuales denunciadas, tipos de estafas electrónicas, zonas afectadas, horario donde más se reflejan las estafas y, de forma transversal, nos introduciremos en un tiempo determinado con los datos adquiridos pertenecientes al segundo semestre del año 2023.

2.1 Población

La población de la presente investigación estará compuesta por las denuncias radicadas por los ciudadanos que resultaron víctimas de estafas virtuales dentro del Departamento San Jerónimo, provincia de Santa Fe, siendo un total de ciento treinta y tres (133). Se analizarán las denuncias recibidas en entidades financieras dentro de la jurisdicción del departamento San Jerónimo, provincia de Santa Fe,

pertenecientes a las ciudades de Coronda, Gálvez, San Genaro, localidades como Maciel, Barrancas y Centeno dentro del segundo semestre del año 2023.

2.2 Marco del muestreo

En este estudio, no se requerirá la ejecución de un muestreo, ya que se analizarán todas las denuncias (siendo un total de 133), recibidas de ciudadanos que resultaron víctimas de estafas virtuales dentro del Departamento San Jerónimo, provincia de Santa Fe. Las denuncias serán asentadas en dependencias dentro de la jurisdicción de las localidades donde se detectaron delitos de esta índole, como son en la ciudad de Coronda, Gálvez, San Genaro, localidades como Maciel, Barrancas y Centeno dentro del segundo semestre del año 2023.

2.3 OPERACIONALIZACIÓN DE LAS VARIABLES

variables	Definición conceptual	Dimensiones	indicadores	indicadores
Estafa virtual	Es un tipo de fraude que se realiza a través de internet, donde se engaña a una persona para obtener información confidencial, dinero u otros beneficios de manera fraudulenta.	La estafa virtual puede tener diversas dimensiones, como l robo de identidad, la suplantación de identidad, el phishing, el fraude en línea, entre otros, es importante estar informado y tomar precauciones para evitar ser víctima de este tipo de delitos.	Tipo de daños, perdida de dinero, robo de información personal, y financiera, daño a la reputación, y posibles consecuencias legales.	victimas
Lugares (jurisdicción) en que se observa un mayor número de denuncias por estafas	Con relación a la población que posee cada ciudad	Numéricas de porcentajes	Comisarías de las ciudades	Víctimas
Franja Horaria	Es un lapso o periodo de tiempo	Desde las 00 hs a las 23.59 hs	Mañana Tarde Noche Madrugada	Madrugada de 01:00 a 07.00 hs Mañana de 07.00 a 13.00 hs Tarde 13.00 a

				20.00 hs Noche de 20.00 a 01.00 hs
sectores vulnerables según el territorio	Sectores o colectividades de individuos que se encuentren en situación de riesgo o desventaja	Edades	De 18 a 35 años De 36 a 50 años Más de 50 años	victimas
Cantidades de contactos telefónicos víctima-victimario	refiere a la cantidad de contactos entre la víctima y el victimario		Si reconoce el nro desconocido	Victimas
Entes utilizados para llevar a cabo el ilícito	Entidad bancaria o benefactora y el delito cometido	Entidades bancarias Entidades benefactoras	Entidad crediticia Unicef Oxfam	Victimas
Valores sustraídos a las victimas	Se refiere al dinero que obtuvo como resultado de un delito	Numéricamente	Montos máximos-mínimos	Victimas
Medios o canales empleados para efectuar el delito	Diversas técnicas de maniobra que usan los ciberdelincuentes para conseguir información del tipo confidencial de los usuarios	Correos electrónicos, mensajes, redes sociales, llamadas telefónicas, visitas en persona	Psíquicas	Victimas
vinculo víctimas y victimario	vinculo que poseen las víctimas y victimarios de un delito	Víctima: persona que sufre un daño, perjuicio o injusticia a manos de otra, grupo o situación Victimario: es la persona que comete un delito o causa daño a otra persona	Lo conoce a la víctima posee datos personales de la misma	Victimas

Fuentes de elaboración propia

2.3 Instrumento de recolección de datos

Total de denuncias	Tipo de delitos	Fecha y hora	Medios empleados para cometer el ilícito	Edad de la victima	Residencia de la victima	Labor de la victima	Comprobante de CBU si se efectuó transferencia	Entidad bancaria con la que opera la victima (CBU)	Nº de veces que la contactaron	Ampliación de denuncia

Fuentes de elaboración propia

TIPO DE ESTAFAS ELECTRÓNICAS

- Phishing
- Smishing (utilización de mensajes de texto)
- Fraude en tarjetas de créditos
- Fraude en transferencias bancarias
- Vishing (mediante la utilización de llamadas o mensajes de voz para obtener información sensible)
- Compras en línea

MEDIOS EMPLEADOS

Pueden cometerse a través de correos electrónicos falsos

Sitios web falsos

Mensajes de textos y llamadas telefónicas engañosas entre otros

FRANJA HORARIA

- Mañana de 07.00 a 13.00 horas
- Tarde de 13.00 a 20.00 horas
- Noche de 20.00 a 01.00 horas
- Madrugada de 01.00 a 07.00 horas

EVIDENCIAS PROPORCIONADAS POR LA VÍCTIMA

- Fecha del hecho
- Número de teléfono desde el cual lo contactaron con las llamadas
- Nombre y apellidos
- Contacto
- vía de contacto
- Motivación de la llamada
- Capital transferido (en caso que se efectuó)
- Canal utilizada (redes, cajero automático, etc)
- Cuentas de destino (número de cuenta, CBU, banco al que responde, datos del titular de la cuenta)
- Comprobantes que corroboren la estafa, como ser: capturas de pantallas de conversaciones u operaciones efectuadas, tickes de movimientos de cajero automáticos, de movimientos de home baking

EDAD DE LAS VÍCTIMAS

- De 18 a 35 años
- De 36 a 50 años
- Mayor 50 años

3 RESULTADOS

Todos los datos adquiridos por la oficina de División Informaciones de la Unidad Regional XV, son plasmados en la presente investigación sobre las estafas virtuales que surgieron durante el segundo semestre del año 2023, dentro el departamento San jerónimo. Según las estadísticas, se indica un aumento repentino en el delito de phishing y sus diversos modos, donde se han registrado 133 denuncias por el delito de Estafas virtuales, las cuales fueron aumentando considerablemente en este periodo, en comparación al primer semestre de ese año.

El phishing se trata de un tipo de ataque cibernético, donde un individuo intenta engañar a las personas, para sí poder obtener información personal, como contraseñas, información bancaria, tarjetas de créditos, haciéndose pasar por una entidad confiable. Estos acontecimientos se pueden dar a través de correos electrónico, mensajes de texto o sitios web falsificados que imitan a compañías legítimas. El objetivo principal del phishing es obtener información confidencial para cometer las estafas, robos de identidad u otros delitos cibernéticos.

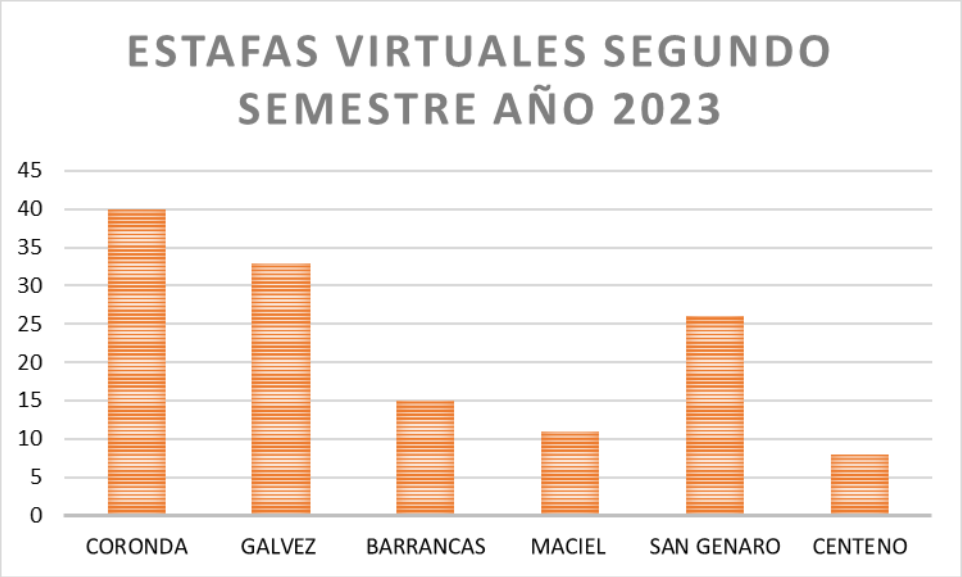
Gráfico Nº 1 tipos de estafas

Fuente: Datos obtenidos de la Unidad Regional XV de Policía

Los delitos por estafas virtuales han aumentado notablemente entre los meses de Julio a Diciembre del año 2023, un 100 % en relación al semestre anterior, siendo

el medio utilizado el internet. Los datos suministrados en el grafico surgen de las estadísticas llevadas por la oficina de División Informaciones perteneciente a la unidad Regional XV, la cual tienen asiento en la ciudad de Coronda. –

Gráfico Nº 2 denuncias asentadas en las distintitas ciudades y/o Localidades, durante el segundo semestre del año 2023

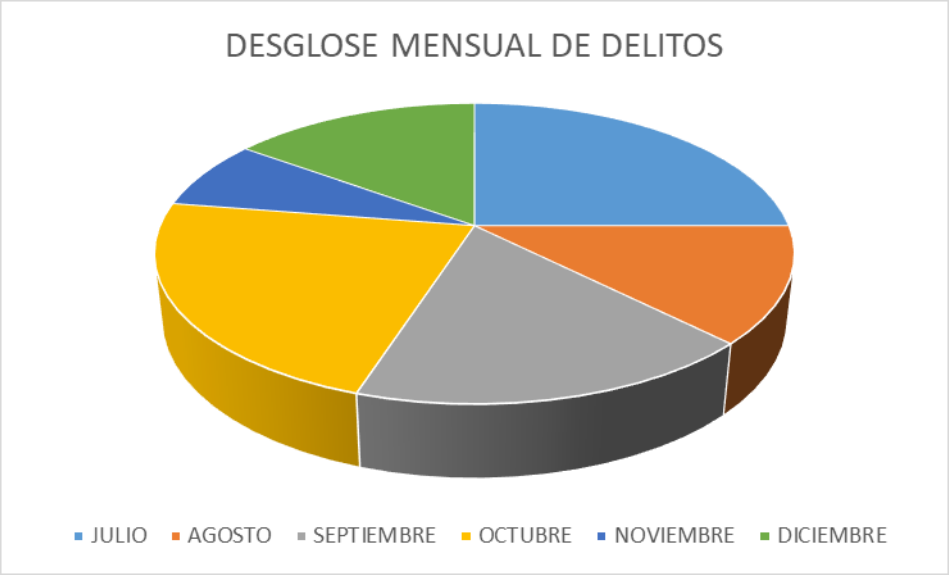


CORONDA	**40**
GALVEZ	**33**
BARRANCAS	**15**
MACIEL	**11**
SAN GENARO	**26**
CENTENO	**8**

Fuente: Datos obtenidos de la Unidad Regional XV de Policía

Durante el segundo semestre del año 2023, se registraron 133 denuncias, por delitos ciberdelitos, un el 30,075 % fueron denunciados en la Ciudad de Coronda cabecera departamental, con un total de 40 casos registrados, en otra ciudad importante, es la Ciudad de Gálvez donde se registró un 24,81 de casos con la cantidad de 33 denuncias, en tanto en la localidades como Barrancas fue de un 11,27 % con 15 casos, Maciel un 8,27 % con 11 casos, San Genaro con un 19,54 % con 26 casos y Centeno con un 6,01% con 8 casos.

Gráfico Nº 3



	CORONDA	GALVEZ	BARRANCAS	MACIEL	SAN GENARO	CENTENO
JULIO	**10**	**8**	**3**	**1**	**5**	**2**
AGOSTO	**5**	**5**	**1**	**0**	**6**	**0**
SEPTIEMBRE	**7**	**9**	**4**	**4**	**4**	**1**
OCTUBRE	**9**	**7**	**2**	**3**	**8**	**1**
NOVIEMBRE	**3**	**1**	**3**	**2**	**1**	**4**
DICIEMBRE	**6**	**3**	**2**	**1**	**2**	**0**

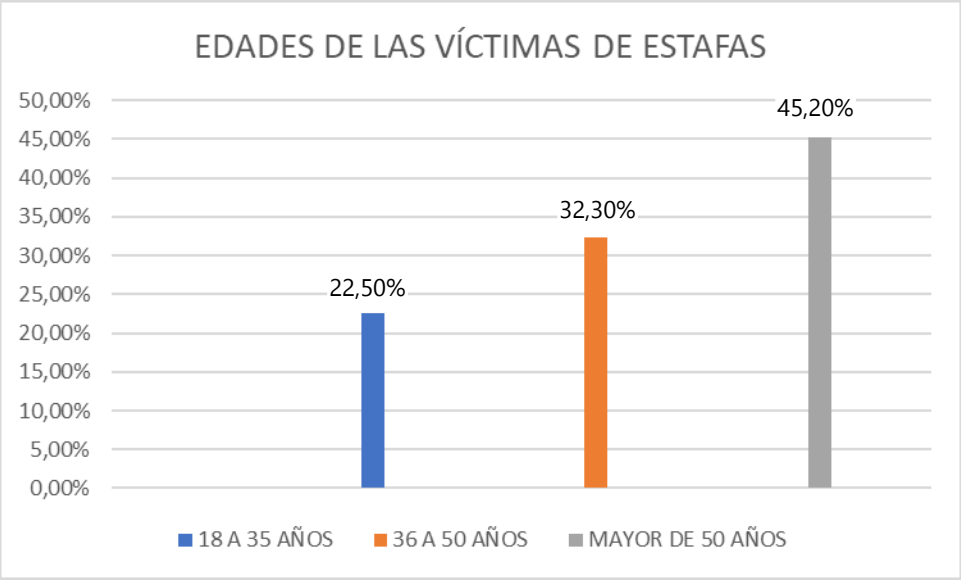
Fuente: Datos obtenidos de la Unidad Regional XV de Policía

Con los datos recolectados de las denuncias asentadas en las diferentes dependencias del departamento San Jerónimo, con conocimiento de la Fiscalia Regional de la Provincia de Santa Fe, se procedió a confeccionar el siguiente gráfico, donde se muestra que las estafas informáticas no, señalan una determinada edad, pero si, se observa que existe gran cantidad de los casos efectuados a personas mayores de edad de 50 años, destacando que de las 133 denuncias radicadas en el segundo semestre del año 2023 en el Departamento San Jerónimo,

60 corresponde a personas que pasan los 50 años, generando esto un crecimiento en la denuncias.

La manera más común de ser víctima de estafas, por parte de una persona mayor, es por medio de la utilización de internet, debido a la falta de familiaridad con la tecnología, a la confianza en a la comunicación tradicional de un llamado telefónico o un correo.

Gráfico Nº 4



Fuente: Datos obtenidos de la Unidad Regional XV de Policía

4. DISCUSIÓN Y CONCLUSIONES

El progreso tecnológico para las personas puede tener un impacto positivo en la sociedad, al mejor la calidad de vida, facilitar el acceso a la información, fomentar la conectividad, impulsar a la innovación y crear empleo, este avance produce una mejora constante en el uso cotidiano de las personas, es decir en su vida diaria. Avances que permiten la disponibilidad y accesibilidad en áreas como la informática, la comunicación, la medicina, la energía, el transporte y muchos otros campos, pero

también se plantean desafíos que deben ser abordados de manera responsable y ética. Ejemplo es el desafío social (brecha digital, la privacidad de datos, el desplazamiento laboral y la dependencia excesiva de la tecnología)

En el presente trabajo se ha investigado en razón de esta nueva modalidad adoptada para la comisión del delito, la cual ofrece numerosas oportunidades a los delincuentes, para cometer una amplia gama de crímenes, lo que requiere de una vigilancia constate por parte de las autoridades y una mayor conciencia por parte de los usuarios para protegerse de estas amenazas en línea. En este caso centramos la investigación en el departamento San Jerónimo, en sus ciudades y/o localidades afectadas, pero la realidad es que estos individuos pueden actuar desde cualquier lugar geográfico, con total anonimato y reserva.

En síntesis, internet es una herramienta eficaz que brinda una variedad de servicios y recursos que han trasformado el modo en que las personas se comunican, acceden a la información, realizan transacciones comerciales, se entretienen, aprenden y colaboran en todo el mundo. Pero debemos aclarar que si es utilizado de forma indebida puede ocasionar daños inesperados, tanto en lo psicológico, como significativos daños económicos.

En Argentina, la ley que trata los delitos informáticos es la Ley 26.388, conocida como Ley de Delitos Informáticos. Esta Ley fue sancionada en el año 2008 y establece disposiciones para combatir los delitos informáticos en el país. La ley define y penaliza una seria de conductas delictivas relacionadas con el uso indebido de sistemas informáticos, como el acceso ilegitimo a datos, la intercepción de comunicaciones electrónicas, la falsificación de documentos electrónicos y el sabotaje informático, entre otros. Además, la ley también establece disposiciones para la cooperación internacional en la investigación y persecución de delitos informáticos.

La investigación aborda la necesidad de que la sociedad adopte una actitud más cautelosa ante la tecnología para impedir ser víctimas de delincuentes informáticos. Se sugiere investigar a fondo las modalidades de fraude utilizadas para educar a las víctimas y reducir los fraudes en aumento. Se recomienda que las entidades financieras efectúen campañas específicas sobre los tipos de fraudes electrónicos y

se sugiere realizar estudios comparativos entre diferentes entidades. Sin embargo, se identificaron limitaciones en la investigación, como el acceso limitado a información por parte de las entidades financieras y la falta de respuesta explicita de las victimas debido a políticas de confidencialidad y posibles sentimientos de temor o vergüenza.

La información reunida permite tener un entendimiento en cuanto a la magnitud del problema y posterior alcance de las conclusiones obtenidas en el presente trabajo. Seguidamente para un mejor abordaje del trabajo se plantean propuestas y sugerencias con una sucesión de medidas a los fines que formen parte de un plan ordenado, los que sean de utilidad para la elaboración de planes estratégicos, a fin de contrarrestar el fraude electrónico existente en el Departamento San Jerónimo, esperando que lo propuesto, no, solo sea de utilidad para este Departamento, sino que también se extienda a otros lugares, donde se origine este delito, para así poder anular estas prácticas que causan importantes pérdidas económicas a las víctimas y sea una herramienta para combatir a los ciberdelincuentes, que día tras día sorprenden a sus víctimas con nuevas formas de engaños. Está claro que este trabajo se enfoca más, en las formas de estafas o fraudes cibernéticos más comunes, como es el phishing, por lo que se proponen pautas para combatir este tipo de delito.

Siguiendo las estadísticas llevadas a cabo por la oficina de División informaciones de esta jefatura departamental, surge que los cometidos mediante la modalidad phishing, son uno de los delitos que más se han acrecentado en los últimos tiempos, donde la tecnología se impone aún más en la vida de las personas, y en todo el mundo debido a los avances tecnológicos. Los diferentes casos se dieron por medio de las redes sociales enviando correos perversos o mensajes engañosos, por lo que, para contrarrestar estos correos maliciosos, surge la necesidad de impartir propuestas para sí, evitar ser víctimas de nuevos ataques:

1. Tener precaución al recibir enlaces, verificar el remitente y hacia donde te direccionan, más aún cuando no has solicitado dicha información.

2. Educar para reconocer señales de phishing, como identificar errores de ortografía, redacción del asunto, en la mayoría de los casos los atacantes no se percatan de la redacción correcta.
3. Utilizar una contraseña robusta o diferente, para cada una de las plataformas y así ir cambiándolas asiduamente.

Otra modalidad de fraude electrónico similar al phishing es el caso del smishing, donde son enviados mensajes de textos a los distintos usuarios de teléfonos móviles por parte de los ciberdelincuentes, empleando métodos intimidantes, es frecuente que estos métodos nos presionen para hacer clic en enlaces o llamar a números desconocidos, enviar códigos, que derivan en vishing para aportar información confidencial, por esta razón debemos estar atento:

1. Para verificar la autenticidad de estos mensajes, es importante comprobar si reconocemos la compañía que los envía y si el remitente es legítimo. Esto obliga inspeccionar cuidadosamente la URL, cotejar la correcta ortografía, gramática y diseños de páginas dudosas.
2. Tener en cuenta las promesas de dinero, es decir que nadie ofrece grandes montos de dinero, o beneficios considerables a desconocidos.

En el caso del delito de vishing (llamadas telefónicas), la mayoría de las personas incurren en una estafa, en razón a que los ciberdelincuentes adaptan sus estrategias a nuestra psicología en el momento. Por ende, es fundamental ejercer precaución para prevenir este tipo de fraude.

1. Evitar entablar conversaciones telefónicas con desconocidos, es el primer paso para evitar una la manipulación que facilite la estafa electrónica.
2. Si en algún momento se mantiene una llamada telefónica con alguna compañía desconocida y en esa surgen dudas o incomodidad, es importante evitar ser amistoso o complaciente, lo correcto es cortar el dialogo de inmediato. En cambio, se puede mencionar que se buscará el número de la entidad y se devolverá la llamada posteriormente, esto permitirá detectar rápidamente si se trata de una estafa.
3. No se debe proporcionar ningún dato personal a través de una comunicación telefónica, a menos que se llame al número real. Nunca se deben suministrar

contraseñas completas, los representantes de las entidades auténticas solo requerirán algunos caracteres.

.

Tanto si se trata de estafas por phihing, vishing o smishing por medio de correos electrónicos, sin importar las tácticas que emplee el atacante para persuadirte de su legitimidad, el estafador dependerá principalmente de la información que proporcionemos de forma voluntaria, Por ende, para evitar caer en una estafa, es crucial no divulgar ningún dato confidencial a menos que se tenga un absoluta certeza o seguridad de que la solicitud es confiable, por lo que si se tiene dudas es mejor abstenerse de proporcionar cualquier dato de interés.

En circunstancias de haber sido víctima de alguna de las tres formas de phishing señaladas, es fundamental:

1. Tomar medidas rápidas, como informar a tu banco o entidad financiera sobre la estafa. Realizar la denuncia correspondiente en la comisaria de jurisdicción o autoridad competente del lugar de residencia.
2. Proceder a cambiar las contraseñas de todas las cuentas en línea que posea, en especial si revelo datos confidenciales, como contraseñas y números bancarios. Conservar las pruebas que posea de los correos recibidos, comunicación mantenida con la persona desconocida que lo contacto, ya que será de ayuda para resolver el caso.
3. Actuar con prontitud para reducir los daños causados por las estafas y proteger tu información personal. Tomar como enseñanza la experiencia vivida para fortalecer tu conciencia y seguridad en línea, como también educar a los demás y a ti mismo sobre reconocer y evitar este tipo de estafas en línea.

5 BIBLIOGRAFÍA.

-Diario Uno Santa Fe -Noticias consultado 22 de Mayo 2024 https://www.unosantafe.com.ar/estafas-virtuales-a72509.html

-GUSTAVO SAIN_ A partir del desarrollo de delios económicos como el espionaje informático, la piratería de software, el sabotaje y la extorsión. En relación al espionaje- https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.

-Historia del Cibercrimen. La primera persona en ser declarada culpable de un delito cibernético fue Ian Murphy, también conocido como Capitán Zap, y eso sucedió en el año 1981_ https://ogdi.org/historia-del-cibercrimen

-ROLANDO ESLAVA –ZAPATA · 2024 — Ley 26.388. (25 de junio de 2008). Delitos Informáticos y Ciberseguridad. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

-RUBINZAL-CULZONI online - RC D. 875/2015- Cibercrimen y Delitos Informáticos. Pensamiento Penal. Ver en: pensamientopenal.com.ar. (4) Sain, Gustavo: "¿Qué son los delitos informáticos?" https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

.

-Registros Estadísticos de la oficina de División Informaciones de la Unidad Regional XV de Policía de la Provincia de Santa Fe. Año 2023.

-Unir- La Universidad en Internet Fraudes por internet, ¿qué tipos de Estafas son más habituales? https://www.unir.net/derecho/revista/fraudes-internet/ consultado 20 de Abril 2024.

APÉNDICE

ÍNDICE DE GRÁFICOS