UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

DELITOS INFORMATICOS EN LAS ENTIDADES BANCARIAS -SUPLANTACION DE IDENTIDAD

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

AUTOR:

MONJA ESQUIVEL GIULIANA MARINA
ORCID 0000-0001-5103-0187

ASESOR:

MG. PÉREZ LÓPEZ JORGE ADALBERTO
ORCID: 0000-0002-4695-389X

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ
ENERO, 2022

Resumen

Mediante este trabajo se busca presentar el crecimiento del delito Informáticos en las entidades financieras bancarias en el Perú cabe señalar que en nuestro país la ley Nº30096 nos indica que mediante esta ley se busca prevenir y castigar los actos delictivos a través de usos tecnología de la información.

La ley Nº30096 (Republica)señala y resguarda la integridad de los ciudadanos en temas cibernéticos por ejemplo información de datos personales, contra el patrimonio, fraudes, suplantación de identidad este último menciona es un delito que está afectando y creciendo en el ámbito de las entidades financieras los Bancos

El tema de suplantación , usurpación o robo de identidad en los últimos años ha tenido incrementos con la tecnología teniendo en cuenta las pérdidas económicas que ha afectado y afecta a los clientes como a las entidades Bancarias ,los facinerosos obtiene y compran información de datos de manera fraudulenta en el mercado negro en algunos casos son cómplices con los trabajadores de las entidades Bancarias para suplantar la identidad de los clientes , causando perjuicios económicos para los usuarios , en este trabajo me enfoco principalmente en el tema de SUPLANTACION DE IDENTIDAD y lo referente que implica este concepto, los casos más comunes son el de tarjeta de créditos , prestamos online comercio electrónico, esta problemática cada día está en aumento .

En este trabajo se busca informar las modalidades de estafa y el perjuicio que ocasiona a los clientes como a las entidades Bancarias.

Palabras clave

Fraude: Engaño económico, acto realizado para eludir o ir contra la, verdad, perjudicando a una o más personas.[1]

Suplantar: Usurpar la personalidad de otra persona.[2]

Banco: Institución Financiera cuyo negocio es invertir o administrar el dinero ajeno, prestar o dar asesoría económica.[3]

Delito: Crimen, violación de ley, acto u omisión, imprudente, sancionada por la ley (languages, 2021).

[1] Diccionario universal unimundo2013
[2] Diccionario universal unimundo2013
[3] Diccionario universal unimundo2013

Abstract

Through this work, we seek to present the growth of COMPUTER crime in banking financial entities in Peru. It should be noted that in our country, Law No. 30096 indicates that this law seeks to prevent and punish criminal acts through information technology uses.

Law No. 30096 (Republic) points out and safeguards the integrity of citizens in cyber issues, for example, information on personal data, against assets, fraud, identity theft, the latter mentioned is a crime that is affecting and growing in the field of entities financial banks

The issue of impersonation, usurpation or identity theft in recent years has increased with technology, taking into account the economic losses that have affected and affect customers as well as Bank entities, criminals obtain and purchase data information fraudulently. in the black market in some cases they are accomplices with the workers of the banking entities to supplant the identity of the clients, causing economic damages for the users. In this work, my main topic is that of IDENTITY SUPPLANTATION and the reference that this topic implies, the most common cases are credit cards, online loans, electronic commerce, this problem is increasing every day.

This work seeks to inform the modalities of fraud and the damage it causes to customers as well as to banking entities.

Keywords

Fraud: Economic deception, act carried out to avoid or go against the truth, harming one or more people.[4]

Impersonate: Usurp the personality of another person.[5]

Bank: Financial Institution whose business is to invest or manage other people's money, lend or give economic advice.[6]

Crime: Crime, violation of law, reckless act or omission, sanctioned by law (languages, 2021).

[4] Diccionary Universasl only world 2013
[5] Diccionary Universasl only world 2013
[6] Diccionary Universasl only world 2013

Tabla de contenido

Introducción

El objetivo de este trabajo es abordar e investigar los delitos informáticos enfocándome en el tema de SUPLANTACION DE IDENTIDAD en las entidades Bancarias Bancos.

Para analizar la problemática de este tema es la preparación y los mecanismo utilizado para obtener los datos necesarios para la suplantación de identidad de los clientes de los Bancos ,las entidades financieras y entidades públicas para controlar y resguardar la seguridad de los ciudadanos han adquirido aparatos modernos e implementados en uso obligatorios de BIOMETRICOS mediante este dispositivo se realiza la identificación de las personas por su huelas dactilares cabe mencionar en los Estados Unidos utilizan el numero brindado de cada ciudadano de seguro social, en el caso de España aplican el uso del identificación brindada por la policía de este país.

La Reniec (Registro Nacional de Identificación y Estado Civil) (rankia, 2019) es un organismo independiente y cada vez se moderniza con la innovación para identificación de los ciudadanos, el 12 de julio de 1995 mediante las ley Nº 264971, sus principales funciones son:

- Emitir el documento Único que certifica la identidad de los ciudadanos peruanos.
- Velar porque se respeten los derechos a la intimidad y identidad.
- Verificación de las firmas.
- Cooperar durante las jornadas electorales.

En nuestro país el Documento Nacional de Identidad DNI ha tenido cambios para resguardar la identidad de las personas, **primero** era el de tres cuerpos , **segundo** el DNI azul tamaño grande, **tercero** el DNI en tamaño pequeño ,**cuarto** el DNI electrónico incluyendo chip la implementación del circuito integrado es utilizado para guardar información y de procesar internamente.

Para incorporar este chip, el DNI cambia su soporte tradicional por una tarjeta de material plástico implementada con modernas medidas de protección en lo cual se innova al antiguo DNI.

Mediante estos cambios y modificaciones su objetivo es proteger la integridad de los ciudadanos para minimizar el tema de suplantación de identidad, los mecanismos de identificación en los países que optan para radicar con el tema se suplantación es la interactuación y el contacto de las personas este tema abarca la identificación física de las personas.

Con la modernización de los medios tecnológicos y uso del internet es fundamental modernizarnos medidas de protección virtuales para la acreditación electrónica para la identificación de las personas con el tema de las firmas electrónicas con la validez que tiene una firma presencial, lamenta mente la falta de información y el interés de los ciudadanos dejan del lado el tema de firmas electrónicas.

podremos utilizarlo para realizar compras firmadas a través de Internet, hacer trámites completos con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas, realizar transacciones con entidades bancarias, participar en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser y muchas otras .

Los Bancos tienen una función muy importante en la actualidad con el tema de la identificación de los clientes para evitar fraudes para sus clientes implementando el uso obligatorio de BIOMETRICOS para realizar pagos como por ejemplo en el Banco de la Nación esta institución ha sido afecta por suplantadores en caso de pago de programas sociales impuesto por el Estado ejemplo Programa Social Pensión 65 y pago de Bono (COVID -19), esta institución ha implementado el uso obligatorio de BIOMETRICOS para los pagos de Programas Sociales , Pago de Subsidios económicos del Estado (Bonos), Pago de Orden Electrónicas del Sector Publico en la mayoría de sus operaciones que se realicen pagos se utiliza ese dispositivo , la institución busca herramientas de protección y seguridad para los clientes con el tema de pagos, los delincuentes han sorprendido usurpando y cobrando bonos brindados por el estado cabe señalar en casos se ha visto que los mismos familiares han usurpado la identidad de los hermanos, padres , sobrinos , cuñados .Las entidades bancarias para poner resguarda a sus clientes han implementado el uso obligatorio de este dispositivo.

En la actualidad las Entidades Financieras Bancos utilizan el dispositivo por medida de seguridad e implementan con información adicional para corroborar la información de los clientes el caso de los datos de Reniec por ejemplo la información que tiene en la base de la Reniec los nombres de los padres, fecha de nacimiento, lugar de nacimiento, grado de instrucción, lugar de domicilio esta información es fundamental para poder identificar a los ciudadanos en los casos que sean necesarios.

Las Medidas de seguridad física perceptibles a simple vista como las tintas ópticamente variables, relieves y fondos de seguridad, o visibles mediante medios ópticos y electrónicos como tintas visibles con luz ultravioleta o micro escrituras; así como medidas de seguridad digitales como encriptación de los datos del chip o acceso al mismo mediante PIN, asegurarían un alto nivel de protección hasta hacerlo prácticamente inviolable o falsificable. Ahora bien, los expertos advierten que el DNI se presenta ya problemas de seguridad de los algoritmos y del entorno, en particular cuando se tiene en cuenta que la mayoría de los titulares carece de conocimientos extensos de informática y apenas adoptan medidas de protección del «hardware» que emplean en el hogar o en el trabajo, lo que los hace más vulnerables a los ataques informáticos orientados a apoderarse de las claves, por ejemplo a través de un virus llamado troyano.

Por lo que se refiere a la seguridad de las tarjetas bancarias y comerciales, sólo en tiempos relativamente recientes la industria ha empezado a investigar el tema, debido a su incremento de uso como medio de pago tanto en el comercio tradicional tanto en el caso de comercio electrónico.

En las operaciones tradicionales es obligatorio la presentación de la tarjeta del cliente titular en lo cual se introduce la tarjeta a un dispositivo terminal en la actualidad se modernizo con la implementación del chip en las tarjetas de crédito, luego se coloca la clave de 4 dígitos del titular previa identificación del cliente con su documento de identidad sea nacional o extranjero(pasaporte , carnet de identidad, Carnet de extranjería) para concluir con la transacción la firma y la verificación .

Los trabajadores de las entidades financieras tienen la obligación de comprobar identidad mediante la foto y la firma, que debe coincidir con la que aparece en el reverso de la tarjeta donde indica para ello. En la actualidad con el tema de la pandemia las entidades Bancarias han optó por tener una verificación de protección más detalladas y requeridas por las entidades para comprobar otros datos para el resguardo de los clientes.

Cabe señalar que en oportunidades los trabajadores de los Bancos no tienen el debido procedimiento de verificación de los clientes, por la aglomeración de clientes se realiza superficialmente la corroboración de los datos como es el caso de las firmas de los titulares, el número de DNI, la fecha de vencimiento de su tarjeta teniendo en cuenta que los datos proporcionados por los clientes en muchos casos son ambiguos y la falta de información de los clientes. En los casos que los clientes no brinden la información se debería solicitar datos para la debida verificación con la ficha de Reniec de los titulares como por ejemplo el nombre de los padres, fecha de nacimiento, lugar de nacimiento, distrito de nacimiento, fecha y año de nacimiento.

En algunos lugares el uso de correo electrónico es utilizado para realizar y corroborar transacciones utilizando el protocolo que se implementó de SMTP facilita las transacciones, pero también es una puerta abierta para los suplantadores y facinerosos siempre teniendo las precauciones del caso. Cuando se utiliza un navegador de internet en algunos casos se solicitan información del titular para que se proceda y se realice la transacción, pero en estos casos no son muy específicos en la verificación de paginas WEB, en la actualidad se incremento un 30% de fraudes electrónicos.

(REPUBLICA, 2021)

La utilización de las herramientas de seguridad para evitar y corroborar la autenticidad y confidencialidad de los servidores no siempre garantiza evitar fraudes a los clientes.

Lo que por un lado facilita el fraude en los lugares de internet los sitios web que permiten la descarga del contenido y, por otro, no impide que un trabajador deshonesto utilice fraudulentamente los datos de los clientes de su tarjeta para obtener lo necesario para realizar operaciones fraude lenta el caso de TOKEN DIGITAL ese dispositivo es utilizado para realizar operaciones como pago de servicio, transferencia de dinero a otros bancos, compra de tiendas virtuales.

Los casos de usurpación de identidad relacionados con el uso de Internet se basan en buena medida en la previa obtención de los datos por medio de ataques a veces muy sofisticados, como el «phishing», el «smishing», el «web spoofing» o el «pharming», y a veces más primitivos, pero en cualquier caso masivos, que son prueba, por una parte, de la enorme capacidad del ciberespacio para llegar a una multitud de víctimas potenciales sin necesidad de una interacción personal y, por otra, de las dificultades que encuentran las Fuerzas y Cuerpos de Seguridad para investigar e evitar actos delictivos relacionadas con las especiales características del medio en que se producen. No hay que olvidar tampoco la extensión en Internet de servicios que permiten crear identidades digitales, como las redes sociales de carácter personal, dando lugar a que muchos usuarios transfieran parte de su vida social a la red. Piénsese en Facebook, Second Life o MySpace, o Tuenti. También se están extendiendo las redes sociales.

Antecedentes

I. Antecedentes nacionales

Aldecoa Jiménez Milagros del rosario, en su tesis (htt1)“El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima ,2019”, la autora describe la importación del internet y la falta de más control del Estado y los retos que tienen el sector financiero , en su tesis señala el tema de SKIMMING es uno de la problemática del día a día y las implementaciones para resguardar la datos de los clientes . La recomendación que brinda en su tesis es la actualización total de la ley Nº30096, la regulación severa de esta ley teniendo en cuenta que no hubo modificación.

En la tesis busca la regularización de los medios informáticos teniendo en cuenta los medios fraudulentos que utilizan los delincuentes para obtener in formación no solo de la persona sino también de las cuentas bancarias y tarjetas de crédito para cometer los actos delictivos.

En esta tesis la autora describe la falta de más impulso del Estado con seguridad tecnológica para los ciudadanos.

Morales Delgado Deivid Yuly, en sus tesis (htt) “La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015” en esta tesis nos habla del tema de la evolución de las tecnologías y la informática que genera incertidumbre y retos para el legislador, como los delincuentes obtiene información de las personas con facilidad.

La autora analiza la legislación y las modalidades que se debe implementar en nuestra norma para obtener una mejoría y no tener un ejemplo que no aporta a la seguridad de los ciudadanos.

La autora recomienda que se brinde una adecuada información del uso de la tecnología de la información para combatir la delincuencia, la participación del pueblo en los temas de tecnología informática, la implementación de herramientas y mecanismos para el personal de la PNP capacitaciones , la participación del Perú en organismos y convenios internacionales para la información y capacitación en delitos informáticos global.

En la tesis se menciona el crecimiento enorme y la problemática de la delincuencia informática que aprende de otros países. La tecnología en la globalización trae nuevos retos, crecimiento como también riesgos y formas delictivas nuevas.

A mi opinión coincido con la autora Aldecoa Jiménez donde recomienda la actualización de la ley Nº30096 para que las sanciones sean mayores, en la tesis de la autora Morales Delgado ella menciona la falta de capacitación de los ciudadanos como el personal de PNP en tema de tecnología a mi opinión es cierto lo que manifiesta porque si hay constante capacitaciones e información la gente está pendiente y en mínima sospecha estaría atento para evitar ser víctimas de los delincuentes.

Es importante las opiniones en estas tesis para conocer la evolución de nuestro país en temas de tecnología y seguridad, teniendo en cuenta que con la globalización nuestro país está en un constante manejo del internet y mecanismos.

II. Antecedentes internacionales

Montaperto ,Javier Eduardo-Argentina en su tesis (htt)“Suplantación de Identidad Análisis sobre su falta de regulación en el ordenamiento jurídico argentino -2018” el autor nos habla la problemática del `país con el tema que sufre los ciudadanos el delito de phishing no ha sido tomada en cuenta en su norma , y él explica en su tesis que la suplantación que no solo es un tema de suplantar identidad si no va de la mano con delitos fraudulentos con delitos de estafa, apropiación de patrimonios, también hace mención que nuestro país está avanzando poco a poco con medidas de protección y la implementación de este delito en su normatividad y que Brasil ,Paraguay y España no tiene un tipo penal específico sobre la suplantación.

Es un tema muy complejo para Argentina el tema de Suplantación también lo consideran como Phishing porque no está regulada en su normatividad dejando sin protección en casos del tema realizando comparación con los países.

El autor igualmente hace mención de la falta de la regularización en la norma de argentina la falta de desinterés de las autoridades acerca del tema.

Hernández Daniel Antonio-Colombia en sus tesis (htp) “La suplantación de Identidad Cibernética en el Ecuador -2019“en su tesis el autor señala la problemática que tiene el país de ecuador en el tema de suplantación.

El nos indica que siendo un país subdesarrollado no le puede brindar las herramientas ni la información necesaria a la población, quedando expuestos para los delincuentes cibernéticos no tiene normas donde regulen el tema.

En esta tesis se recomienda la ecuación del usos de los medios informáticos y creación de normas que regulen con mayor enfoque del tema , la constante actualización de sus funcionarios en tema de delitos cibernéticos para poder buscar medidas de protección para los ciudadanos

Las dos tesis tienen aportaciones importes en el tema de suplantación en otros países y las recomendaciones brindadas en otro enfoque , la tesis del autor Hernández Daniel tiene una perspectiva del País de Ecuador acerca del tema de suplantación la falta de capacitación que genera que los ciudadanos se encuentre vulnerables , si los países no tienen una adecuada respaldo para el tema de suplantación imaginemos como serán al momento que las instituciones Financieras Bancos quieran optar por medidas que resguarden la protección de sus clientes, la falta de modernidad , tiene aportaciones importantes con el déficit que tiene cada país con el tema de Suplantación.

Cabe mencionar que estos trabajos de investigación tienen aportaciones importantes en el tema de investigación, teniendo un concepto de los demás países como se ha desarrollado con el tema de suplantación de identidad ,las recomendaciones que dan cada autor para su país.

Marco Teórico

I. Antecedentes

La suplantación o robo de identidad en internet consiste en hacerse pasar por otra para cometer actividades delictivas, tales como fraude o estafas, obtener datos o información sensible o confidencial.

La mayor o menor facilidad para hacerse con los datos necesarios para suplantar la identidad de una persona realmente existente depende en buena medida de la estructura que presentan los mecanismos de identificación de la persona en cada país y de sus puntos vulnerables, que no son creados sino aprovechados por los delincuentes. Así, por ej., el hecho de que en los Estados Unidos se utilice como dato identificativo fundamental el número de la seguridad social (SSN, Social Security number), que no nació con dicho propósito, sino para mantener un adecuado registro de las ganancias.

En la actualidad, las medidas adoptadas contra la falsificación van desde la impresión de la palabra «España» con una tinta ópticamente variable, que se magenta o verde al variar el ángulo de observación, hasta un hilo de seguridad, embebido en el papel, que cruza en sentido vertical toda la superficie del DNI y es luminiscente a la luz ultravioleta, pasando por fondos de seguridad para la fotografía en color del titular y la grabación del número del DNI en láser, apreciable al tacto. Pese a estas medidas, existen infinidad de casos de falsificación del DNI, sea mediante la alteración de uno legítimo, los menos, sea mediante la elaboración de uno con datos falsos.

Los mismos problemas que surgen en el DNI tradicional afectan al pasaporte, al número de Identificación de Extranjero (NIE), a los permisos de residencia y de

trabajo, etc. Ninguno de estos documentos de identificación es completamente seguro.

A ello se añade que la mayoría de los mecanismos de identificación y autenticación desarrollados en el mundo real, basados fundamentalmente en el contacto personal entre los sujetos que interactúan y el reconocimiento de la apariencia física o de la firma, no son aplicables al mundo virtual. Por ello, con la llegada de la Sociedad de la Información y la generalización del uso de Internet se consideró necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad con el fin de poder acreditar electrónicamente y de forma indubitada la identidad de la persona, y que pudiera firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita. Para responder a estas nuevas necesidades nació el Documento Nacional de Identidad electrónico (DNI), regulado por el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar información y de procesarla internamente. Para incorporar este chip, el DNI cambia su soporte tradicional (cartulina plastificada) por una tarjeta de material plástico, dotada de nuevas y mayores medidas de seguridad.

En la medida que el documento nacional de identificación(DNI) se vaya modificando para el DNI tradicional y se implanten las nuevas aplicaciones, podremos utilizarlo para realizar compras firmadas a través de Internet, hacer trámites completos con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas, realizar transacciones con entidades bancarias, participar en una conversación por Internet con la certeza de que nuestro interlocutor es el titular.

Por añadidura según lo mencionado todo abarca en este tema los implicados en su desarrollo este novedoso sistema de identificación resulta virtualmente imposible de falsificar, tan diversos son los elementos que lo constituyen.

Medidas de seguridad física perceptibles a simple vista como las tintas ópticamente variables, relieves y fondos de seguridad, o visibles mediante medios ópticos y electrónicos como tintas visibles con luz ultravioleta o micro escrituras; así como medidas de seguridad digitales como encriptación de los datos del chip o acceso al mismo mediante PIN, asegurarían un alto nivel de protección hasta hacerlo prácticamente inviolable o falsificable. Ahora bien, los expertos advierten que el DNIe presenta ya problemas de seguridad de los algoritmos y del entorno, en particular cuando se tiene en cuenta que la mayoría de los titulares desconocen conocimientos extensos de informática y no utilizan las medidas de protección del «hardware» que emplean en el hogar o en el trabajo, lo que los hace vulnerables a los ataques informáticos orientados a apoderarse de las claves, por ejemplo a través de un troyano o de un «keylogger»

Por lo que se refiere a la seguridad de las tarjetas bancarias y comerciales, sólo en tiempos relativamente recientes los bancos toman medidas de seguridad y protección para evitar fraudes electrónicos contra los clientes.

Con la modernización en todos los aspectos, las entidades financieras buscan frenar con los delincuentes cibernéticos y suplantadores de identidad implementando sus herramientas de seguridad en algunos casos tienen seguros en los cuales cubren robos y phisning (fraude cibernético). El tema de suplantación es muy complejo porque en muchos casos en los lugares alejados no se aplican las herramientas necesarias, la falta de interés de los clientes por informarse e investigar los delitos informáticos. En la actualidad el incremento de suplantación de identidad se ha incrementado en todo el Perú en los mayores casos son en provincia.

El caso de un cliente que denuncio que realizaron un retiro de su cuenta bancaria por el importe S/20.000 en provincia cabe señalar que el cliente radica en lima, pero los suplantadores realizaron el retiro en provincia, por son mas vulnerables sus herramientas que tienen los bancos por la falta de internet (FIBRA OPTICA), pagina de Reniec, y otros. El caso de la clienta que realizaron una transferencia a otro banco con el dispositivo de TOKEN DIGITAL mediante claves por mensaje de textos en otros casos los trabajadores del banco están confabulados con los delincuentes para realizar los actos delictivos.

Doctrina

- Gómez Mendoza, Gonzalo (2005). Delitos privados contra el honor. (Ed 2005). Lima Perú.

- Reyna Alfaro, Luis (2002). Los delitos informáticos: Aspectos criminológicos, Dogmáticos y de política criminal. (1 Ed). Lima – Perú

Jurisprudencia

- **Casación N 363-2015-Santa**, señala que el señor Hernan Lopez Huaman usurpo la identidad de su hermano Javier Lopez Huaman para realizar los actos delictivos en una entidad financiera.

- **Casación Nº828-2014-Lambayeque** señala nula las sentencias de la primera y segunda instancia a fin de garantizar la garantía constitución.

Conclusiones

A mi opinión el tema que he tratado en el siguiente trabajo tiene una aportación importante para nuestra sociedad y país, me realizo la siguiente interrogante:

¿Qué es el robo de identidad? “El robo de identidad es cualquier clase de fraude que dé como resultado la perdida de datos personales, como, por ejemplo contraseñas, nombres de usuario, información bancaria o números de tarjetas de crédito. El robo de identidad en línea en ocasiones se conoce como la suplantación de identidad.

El robo de identidad no es nuevo. Los ladrones siempre han encontrado maneras de apropiarse ilegalmente de la información personal mediante engaños (también conocidos como ingeniería social), robando el correo electrónicos e incluso revisando los cubos de basura. Ahora que el robo de identidad se ha trasladado al Internet, los delincuentes pueden engañar y se hacen vulnerables los clientes en su información y la falta de información de los clientes en los temas de fraude.

Como nos han dicho nuestros amigos de Microsoft, el robo de identidad no es nuevo los ladrones siempre van a encontrar ese agujerito por donde meterse para robar cualquier cosa, en este caso nuestra información, y lo hacen por métodos como la ingeniería social.

En épocas anteriores estos ACTOS DELICTIVOS se han usado la modalidad hablando por teléfono, yendo directamente con la persona o empresa a la que le querías sacar información y convencerla por medio de engaños, revisando cubos de basura o simple y sencillamente espiando.

En la actualidad los delincuentes buscan herramientas para sus actos delictivos, estos delincuentes dándoles un arma más para atacarnos que son las redes sociales. “La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harán.

El tema de la tecnología Mundialmente ha traído aportaciones positivas y negativas para la humanidad cabe mencionar que cada país ha tomado las medidas de seguridad en caso de delitos informáticos que con lleva el tema de suplantación de Identidad, en nuestro país las autoridades han tomado medidas y normas para castigar casos.

Lastimosamente algunos países no están preparados ni implementan medidas de protección en dicho tema es el caso de argentina cabe mencionar que los países europeos tienen medidas de protección avanzadas en comparación de países latinoamericanos (países subdesarrollados).

El Perú en comparación de otros países a desarrollado medidas de protección en el tema de delitos de informática(suplantación de Identidad), el cambio de documento de identidad DNI, en la actualidad el DNI biometrico.

Recomendaciones

- Lo bancos tiene que utilizar de forma obligatoria el uso de biométricos para la identificación de los clientes, optar por herramientas de seguridad países expertos en estos casos.
- Capacitar al personal en temas de delitos informáticos.
- Invertir en capacitadores extranjeros en temas de suplantación de identidad.
- Trabajar de la mano con el ministerio de interior con el personal de PNP para le detención de usurpadores.
- Las penas por el delito tienen que ser mayores su condena.
- Informan constantemente a los ciudadanos de los riesgos que tienen y capacitar para evitar pérdidas, fraudes y robos cibernéticos.
- Implementar herramientas y software en las entidades financieras BANCOS para la protección de los clientes.
- Enfocarse en las ciudades más remotas las capacitaciones constantes de fraudes Electrónicos.
- Evaluar el tema de adquirir fibra de óptica para los BANCOS.
- Realizar evaluaciones constantes psicológicas al personal.
- Reforzar el área de tecnología en los Bancos para mejor e implementar medidas de protección.

- Evaluación en el perfil del personal de área de Tecnología y servicio al cliente.
- Evitar obligatoriamente el uso de celular en las entidades financieras.
- Solicitar apoyo a los países desarrollados en capacitación personal idóneos en el tema.
- La renovación de los equipos de Biométricos en las entidades Bancarias de provincia.

Bibliografía

- Diccionario universal unimundo2013
- www. Gaceta jurídica.com.pe
- vlex.com.pe
- Articulo de Periódico La Republica 2021.
- htps:// Alicia.concytec.gob.pe
- https://bdigital.uexternado.edu.com
- https://gestion.pe
- Articulo de Periódico Gestión 2021