TECNOLÓGICO NACIONAL DE MÉXICO

TESCHA
TECNOLÓGICO DE ESTUDIOS SUPERIORES CHALCO

INGENIERIA EN INFORMATICA

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHALCO

“Los 4 Principales Tipos De Fraude Cibernético En México

”

INTEGRANTES:

Soriano Santiago Jahaira Ibeth

Velazquez Carmona Laura Alexia

Zavala Coronado Adaneli

DOCENTE:

Kevin Gyovani Ramírez Vite

Resumen

Este artículo da una mirada general acerca de los 4 principales tipos de fraude cibernético en México su definición y su implicación en la forma como se trata la información en México. Además, muestra la importancia de la seguridad en, el robo de datos de tarjetas bancarias, phishing, envió de recibos bancarios falsos, instalación de software malintencionado y su puesta en práctica de manera efectiva, de la mano con diferentes herramientas tecnológicas. En definitiva, explica su aplicación, así como la legislación existente en materia de delitos informáticos en nuestro país.

Palabras claves: delito informático, phishing, seguridad, software, robo de identidad, bot nets, phishing, fraude de afiliación.

INTRODUCCIÓN

México actualmente ha pasado por diversas transiciones tecnológicas en múltiples áreas de la vida cotidiana, como escuela o entretenimiento sin embargo un área de relevancia es la bancaria o aquellas donde se guarda información sensible, las cuales en la última década han avanzado a pasos agigantados pues cada vez es mas común que en vez de ir a una sucursal bancaria puedas realizar algún tramite o requisito a través de la aplicación del banco o que puedas respaldar tus fotos, o guardar documentos a través de un servicio de nube, estas prestaciones han crecido exponencialmente, pero a la par de ese crecimiento se encuentran riesgos presentes en todo momento.

Como ya dijimos los servicios de bancos o de información han evolucionado para hacer operaciones a través de internet, o guardar información sensible de una

persona, hacer compras en línea etcétera, sin embargo, al tratarse de dinero o información valiosa, se presentan riesgos latentes, en los cuales una persona puede caer inadvertidamente y perder su dinero o que su información sensible sea usada para fines inmorales o algo peor.

Estos riesgos se denominan como fraudes cibernéticos, los cuales son muy variados dependiendo del objetivo del defraudador, así como la manera en que alguien es engañado para caer en estos, en el presente articulo se abordan los principales 4 fraudes cibernéticos que se presentan en México, de acuerdo a David Corella Ramírez quien realizo una aportacion en la revista digital de tecnologias informáticas y sistemas donde se muestran algunos de los temas ya mencionados como son: el phishing, recibos bancarios falsos, software malintencionado, y robo de datos de tarjeta, todos presentes en nuestro día a día y que debemos conocer para poder protegernos y cuidarnos de mejor manera al usar los servicios que actualmente se nos proporcionan en internet.

1. Phishing

“Se define como un tipo de malware o un término para que alguien envía un correo electrónico falsificado a las víctimas al azar para tratar de obtener información personal sobre ellos. Más específicamente en la informática, el phishing es una actividad criminal utilizando técnicas de ingeniería social para adquirir fraudulentamente información sensible como nombres de usuario y contraseñas, tratando de engañar a los usuarios de sitios web populares enviándolos por correo electrónico versiones falsas de la web para dar a sus credenciales.” (Bernal, 2019)

El Phishing es un problema que afecta actualmente a todo tipo de personas, robando información confidencial como nombres de usuario, contraseñas e

información de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

La mayoría de los ataques de Phishing comienzan con un correo electrónico que afirman que se ha emitido por una empresa de confianza. Este correo electrónico anima al usuario a hacer clic en la dirección que se proporciona en su contenido. Esta dirección se dirige al usuario a una página web ilegal, que está diseñado a un sitio web válido supuestamente, por ejemplo, el sitio de un banco o una institución financiera.

Imagen 1. Phishing

El fraude cibernético más común en México es el phishing pues este opera de formas diferentes los ciberdelincuentes usan una variedad de métodos para engañar a los clientes que buscan información en empresas.

Phishing y Pharming: dos formas de suplantación de identidad. En el phishing, el delincuente cibernético consigue engañar al usuario mediante un correo, normalmente ‘spam’, invitándole por ejemplo a realizar una operación bancaria en una página que aparentemente tiene la misma interfaz que la de su banco. Por el contrario, en el Pharming no es necesario que el usuario efectúe una operación bancaria accediendo a la página mediante un link que le proporciona el timador. El usuario intentará acceder directamente desde su navegador con la normalidad de siempre, excepto en que la página a la que acceda será una copia de la original. (David Corella Ramírez, Tipos de Fraudes en mexico, 2019)

En este texto se hace una pequeña comparación acerca de phishing y Pharming así mismo como se hacen uso de las mismas con un pequeño ejemplo de cada una el son una modalidad de engañar a nuevos usuarios.

Imagen 2. Principales delitos cometidos en Internet del tipo 1

TIPO 1	**ROBO DE IDENTIDAD**
	Phreaking (especialistas en mecanismos para vulnerar la seguridad de los sistemas telefónicos)
	AMENAZAS
	Fraudes en e-commerce (portales de subasta)
	FRAUDES EN LÍNEA (COMPRAS EN TIENDAS VIRTUALES)
	Clonación de tarjetas de crédito
	ROBO DE INFORMACIÓN
	Carding (utilización ilegal de tarjetas de crédito)
	TRASPASOS ILEGÍTIMOS
	Phishing (correos falsos para robar datos de usuarios)

2. Envió de recibos bancarios falsos

“En la actualidad nos encontramos ante la presencia de una tendencia de la actividad jurisdiccional encaminada a acudir a criterios objetivos de responsabilidad de los establecimientos bancarios por el incumplimiento de sus obligaciones contractuales, con el fin de proteger al consumidor financiero, como sujeto de especial protección por parte del ordenamiento jurídico. Tal vez uno de los casos más emblemáticos de los que se enmarcan en dicha tendencia es el de la responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados, que cuenta con un régimen legal que permite distinguirlo del régimen general de responsabilidad de dichas entidades, razón por la cual se hace necesario su estudio y análisis” (Jorge Alberto Padilla Sánchez, 2017)

se crean muchos cheques falsos a esto los bancos tienen la responsabilidad de proteger la información tanto personal como bancaria de sus clientes esto con el objetivo de no caer en fraudes cibernéticos.

“Ciberdelincuentes, como ahora les llaman, clonan portales electrónicos con la imagen corporativa de reconocidas empresas y ofertan desde ahí flotillas y automóviles en remate supuestamente propiedad de grandes corporaciones tanto públicas como privadas, que usan como gancho para atraer víctimas y defraudarlas con miles de pesos. Es una modalidad de fraude cibernético transnacional operada con Internet en el ciberespacio. Robo de identidad: el robo de identidad es cualquier clase de fraude que origine la pérdida de datos personales: contraseñas, nombres de usuario, información bancaria o números de tarjetas de crédito.”

En la actualidad existe el robo de tarjetas bancarias haciendo mal uso del robo de identidad de las mismas esto es una modalidad que no solo opera en México, sino que también lo hacen en todo el mundo y es más común de lo que se cree.

Imagen 3. Robo de tarjeta (skimmers)

3. **Instalación de software mal intencionado**

   Existen diversos tipos de estos, con diferente denominación, las cuales se mencionan a continuación:

   1) Bot nets: Son robots informáticos que se instalan en nuestros ordenadores, mediante spam o malware. El estafador de este tipo de

fraude online suele estar en un país con compras vetadas en comercios electrónicos, por lo que utiliza IP de otros países para no levantar sospecha. Su rastro es bastante complicado de seguir, aunque se estima que puede haber más de tres millones de este tipo de especialistas por la red.

2) Re-shipping: un defraudador compra en un comercio electrónico con una tarjeta robada y utiliza una mula, personas que recibirán la mercancía a cambio de una comisión, para evitar ser descubiertos. Una vez recibida, la mula se la envía al defraudador.
3) Fraude de Afiliación: Consiste en lanzar una campaña de muchos productos a un descuento muy bueno, imitando a los programas de afiliación más conocidos, pero el programa de afiliación es falso.
4) Robo de identidad: el robo de identidad es cualquier clase de fraude que origine la pérdida de datos personales: contraseñas, nombres de usuario, información bancaria o números de tarjetas de crédito.
5) Fraude amigo: Se recibe una compra, se hace todo correcto, Se entrega la mercancía, pero pese a que todo parecía normal a los pocos días se recibe una devolución. ¿Qué ha pasado?, pues que el cliente ha declarado la compra como fraudulenta en su banco, aunque en realidad fue él quien hizo la compra.

Imagen 4. El lado oscuro del internet, clasificación de los delitos cibernéticos

SYMANTEC	POLICÍA CIBERNÉTICA	DESCRIPCIÓN
Tipo 1	Delito Cibernético	Es el robo o manipulación de datos o servicios por medio de piratería o virus, el robo de identidad y fraudes en el sector bancario o del comercio electrónico
Tipo 2	Delito Cibernético que afecta a la sociedad	Son actividades como el acoso en internet, turismo sexual, extorsión, chantaje, espionaje, terrorismo, abuso de menores, explotación sexual comercial infantil, robo o sustracción de menores, etc.

Los resultados obtenidos están dedicados a mostrar el delito tipo 1, apoyando la comprobación de páginas electrónicas que están dedicadas exclusivamente a este tipo de fraudes y que permitan descifrar la manera de operar de dichas organizaciones delictivas.

4. Robo de datos de tarjetas

En México, el delito de robo de tarjetas va en aumento día con día, según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, el robo de identidad se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria. Comúnmente, el delito de robo de identidad se usa de manera ilegal para abrir cuentas de crédito, contratar líneas telefónicas, seguros de vida, realizar compras e incluso, en algunos casos, para el cobro de seguros de salud, “Uno de los indicadores del robo de identidad es el reporte generado por la Comisión Nacional Bancaria y de Valores. de operaciones monetarias realizadas por los clientes, agrupadas por productos y canales transaccionales de las Instituciones. La luz de la metodología CRISP-DM, con lo que se puede fortalecer el combate a estos delitos”. (Hernández, 2018)

Imagen5. Robo de datos con tarjeta de crédito

El fraude electrónico en cajeros automáticos (ATMs) ha sido uno de los vectores más explotados dentro de las entidades financieras, destacándose por su crecimiento en los últimos tiempos.

Existen diversas técnicas con las cuales los ciberdelincuentes logran hacerse de una copia de la banda magnética correspondiente a una tarjeta de crédito o débito,

la cual es utilizada para consumar un hecho delictivo, realizando compras o directamente retirando dinero de cuentas bancarias.

En este caso profundizaremos en una técnica que implica la utilización de skimmers, para duplicar bandas magnéticas de tarjetas de crédito, para realizar fraudes financieros. Esta práctica es muy utilizada en todo el mundo debido a que suele darles buenos resultados a los cibercriminales, es de fácil adquisición y rápida implementación, envíos de recibos bancarios falsos fraude con tarjetas de crédito y débito**:** El fraude con tarjetas de crédito y débito es otro problema grave en México. Los delincuentes pueden obtener los detalles de las tarjetas de forma ilegal a través de técnicas como la clonación de tarjetas o el robo de información en puntos de venta comprometidos, una vez que obtienen los datos de la tarjeta, realizan compras fraudulentas en línea o retiran dinero de cajeros automáticos, causando pérdidas económicas a los titulares de las tarjetas y a las instituciones financieras

El fraude con tarjetas de crédito y débito en el entorno virtual de los negocios de la ciudad de Pucallpa en donde México se encuentra involucrado con los distintos fraudes en los últimos años se ha incrementado significativamente que afectan a clientes de diferentes entidades bancarias y financieras, lo que genera incertidumbre y desconfianza en operaciones ante cajeros automáticos, por ello como objetivos específicos se ha analizado la relación entre el fraude por robo de datos en cajeros automáticos y la aceptación de la colaboración de personas particulares en la manipulación de tarjetas atascadas, por otro lado se ha determinado la relación que existe entre el fraude telefónico de supuestos empleados bancarios y la obtención de datos confidenciales de clave token digital, clave de cajero, que otro de los problemas que afectan a muchos clientes, por ello en la investigación se establece la relación existente entre el fraude por clonación de tarjetas por operaciones comerciales y la falta de protección de clave de tarjeta o no solicitar el POS. (Rodriguez Ruíz & Ruíz Torres, 2022)

El fraude con tarjetas de crédito y débito es otro problema grave en México. Los delincuentes pueden obtener los detalles de las tarjetas de forma ilegal a través de técnicas como la clonación de tarjetas o el robo de información en puntos de venta

comprometidos. Una vez que obtienen los datos de la tarjeta, realizan compras fraudulentas en línea o retiran dinero de cajeros automáticos, causando pérdidas económicas a los titulares de las tarjetas y a las instituciones financieras. (ESET, 2015)

RESULTADOS

El objetivo de la presente investigación fue Analizar los 4 principales tipos de fraude cibernético en México se utilizó la metodología descriptiva, el análisis de artículos, tesis, revistas tecnológicas y páginas web. Los resultados obtenidos advierten que el ilícito de fraude informático comparte los mismos fraudes cibernéticos como los son el phishing, envió de recibos bancarios falsos, instalación de software malintencionado y el robo de datos de tarjetas. Finalmente se concluye que el delito de fraudes cibernéticos puede ser considerado como un hurto cometido por medios informáticos y que el delito de acceso ilícito puede ser sancionado.

CONCLUSIÓN

Con este articulo se ha pretendido dar una breve explicación acerca de los fraudes cibernéticos para que el publico en general tenga en cuenta los riesgos que tiene al compartir su información tanto personal como bancaria en páginas web ilícitas o simplemente dando clic en los enlaces enviados por correos electrónicos no confiables.

BIBLIOGRAFIA

Referencias

A. B. (12 de enero de 2018). *googlo academico*. Obtenido de http://paginaspersonales.unam.mx/app/webroot/files/1406/Publica_20230202225725.pdf

Bernal, M. L. (2019). protocolo para la prevención de ataques de phishing . *Revista Digital de tecnologias informáticas y sistemas* , 3-3.

David Corella Ramírez, A. G. (2019). Tipos de Fraudes en mexico. *Revista Digital de tecnologias informáticas y sistemas*, 6-8.

David Corella Ramírez, A. G. (2021). Modalidades de fraude en la compra-venta de artículos por medio de aplicaciones electrónicas. *Dialnet*, 72-79.

ESET. (2 de Abril de 2015). *ESET*. Obtenido de https://www.welivesecurity.com/la-es/2015/04/06/qu-es-skimmer-como-proteger-targeta/

Rodriguez Ruíz, Y., & Ruíz Torres, S. L. (2022). *google academico*. Obtenido de http://repositorio.unu.edu.pe/handle/UNU/5340

Vayansky, S. K. (2018). phishing, retos y soluciones . *fraude y seguridad informatica* , 6.