VICERRECTORÍA ACADÉMICA
DEPARTAMENTO DE CURSO MONOGRÁFICO

Trabajo Final de Grado para optar por el título de Ingeniería en Sistemas de Computación

Título de la monografía:

"Análisis de las principales técnicas para usurpación de identidad para la obtención de datos de tarjetas de crédito y débito en la República Dominicana, año 2020-2021."

Sustentantes y matriculas

Edgar Omar Ferreras Marrero	A00096697
John Tomas Medina Aquino	A00094476
Carlos Manuel Rosario Aquino	A00093352

Asesor:

Willy Alfredo Padua Ruiz

Coordinación Curso Monográfico: Dra. Sención Raquel Yvelice Zorob Avila

Distrito Nacional, República Dominicana

2021

Agradecimientos

A **Jehová Dios**, y a nuestro señor **Jesucristo**, por darme las fuerzas, conocimiento, fortaleza y poder para llegar a esta etapa tan importante en mi vida.

A mi madre, **Lupe Marreo**, mi gran amor, mi columna y uno de mis mayores ejemplos y razones de ser, gracias por el amor incalculable, me faltan palabras para describirte; Mas hoy te dedico este título con regocijo. ¡Tu hijo pudo lograrlo!

A mi padre, **Oscar Ferreras**, sin lugar a duda mi ejemplo de que haciendo las cosas bien podemos llegar a ser grandes, y de que podemos superarnos. Gracias por tantos consejos, por ser un excelente padre y por toda tu dedicación. ¡Te amo!

A mi pequeño hermano, **Eddy Rafael**, el cual amo y me siento orgulloso, espero ser un ejemplo para ti.

A mi pareja, **Arlyn García**, no tengo palabras para agradecerte, mi apoyo incondicional, mi amiga y consejera, la que a pesar todo siempre está aquí, para mí es un orgullo estar a tu lado.

A mi amigo, **Carlos Ulloa**, el cual es un hermano para mí, gracias por estar aquí cuando te necesito, gracias por tus consejos y gracias por la gran persona que eres.

A mi familia y amigos que me apoyan y me dan la mano siempre que necesito de ellos, por los memorables momentos y los que aún faltan, gracias por creer en mí y alentarme a seguir creciendo, en especial mención a: **Isabel Mejía, Abricio Ferreras, Petra Ferreras, Aníbal Montero, Belkis de la Rosa, Omar Mejía, Martha Mejía, Dimayo Mejía, Leandro García, Griselda Matos, Yokasta Matos, Andrés Jaqués, Kenia García, Juan García, Oscar Ferreras (hijo), Paola Ferreras.**

A mis compañeros de monográfico, **John Medina** y **Carlos Rosario**, gracias por la confianza, el apoyo y la dedicación para llevar a cabo este proyecto. Por esas noches largas que si han valido la pena. A todos mis amigos de la universidad.

A nuestro asesor **Willys Padua** por su paciencia y dedicación, y por enseñarnos tanto. A todos mis profesores también que de todos me he llevado algo.

Por último, y no menos importante, mi **Universidad Acción-Pro-Educación y Cultura (UNAPEC)** por ayudarme a crecer y desarrollarme. Por las experiencias y momentos inolvidables que en ella pase. Por las personas que allí conocí que hoy en día son amigos que aprecio.

A veces podemos encerrarnos y creer que estamos lejos de alcanzar lo que soñamos, pero el tiempo de Dios es perfecto, y él nos ayuda a superar las adversidades. Gracias a todos los que me apoyaron en este largo, tedioso, pero a la vez maravilloso camino. Gracias a todos.

Edgar Omar Ferreras Marrero

Agradecimientos

Primeramente, gracias a **Dios** que me ha estado acompañando a lo largo de este viaje, permitiéndome y ayudándome a estar en el lugar donde estoy.

A mi madre, **Fior Aquino**, por su apoyo incondicional, por su esfuerzo en enseñarme el mejor camino para mí, por ayudarme a estudiar en las noches de velo, por los consejos dados que me permitieron alcanzar esta meta, sobre todo por ser mi madre y estar ahí siempre para mi sin poner excusas ni pretextos. Este título es dedicado a ti, Te amo muchísimo.

A mi padre **Tomas Medina**, por ser un padre ejemplar, un ídolo y enseñarme lo bueno y lo malo, por el apoyo y los consejos, por ser mi padre Gracias.

A mi hermana, **Chelsy Medina** para la cual he sido un ejemplo de que, si podemos lograrlo, te amo niña.

A mi hermano pequeño, **Geysell Medina** el cual es mi inspiración y del cual espero sentirme orgulloso, te amo niño.

A mi abuela, **Rufina Veloz**, por ayudarme siempre y brindarme un apoyo incondicional.

A mi familia, amigos y personas que me apoyan o apoyaron, que en algún momento de esta carrera universitaria me brindaron su apoyo, muchas gracias a todos, gracias por creer en mí, en darme ese empujón que muchas veces necesite, mención especial: **Soraine Aquino, Emely pantaleon, Fausto Santos, Moises Tavarez, Elizabeth Aquino, Wellington Aquino, Alex Aquino, Jeffry Rodriguez.**

A mis exparejas y pareja actual, que aportaron su grano de arena para poder llegar a la meta de esta carrera, a ustedes también muchas gracias.

A mis compañeros de monográfico, **Edgar Ferreras** y **Carlos Rosario**, gracias por la confianza, el apoyo y la dedicación para llevar a cabo este proyecto. Por esas noches largas que si han valido la pena. A todos mis amigos de la universidad.

A nuestro asesor **Willy Padua**, por su dedicación y apoyo para llevar a cabo este proyecto.

Al profesor **Mario Luciano**, que gracias a el pude descubrir la rama informática que me apasiona y que ahora disfruto tanto.

Por último, y no menos importante, mi **Universidad Acción-Pro-Educación y Cultura (UNAPEC)** por ayudarme a crecer y desarrollarme. Por las experiencias y momentos inolvidables que en ella pase. Por las personas que allí conocí que hoy en día son amigos que aprecio.

Siempre podemos lograr lo que nos proponemos si le ponemos empeño, podemos lograr nuestro sueño, en mi caso desde el año 2015 era mi anhelo, gracias al amor y empeño que le aplique estamos aquí. Gracias a todos los que en algún momento compartí clases, gracias a los que nos juntamos en la biblioteca a estudiar, gracias a nuestros maestros. Gracias a todos.

John Tomas Medina Aquino

Agradecimientos

Primero a Dios las gracias por haberme brindado todas las fuerzas para subir cada escalón que se presentaron en el camino para continuar con mi carrera hoy en día y permitirme llegar donde estoy a ver todo lo que es logrado que en primer lugar sin ti ni tus inmensas bendiciones no lo hubiese logrado.

A mi madre, **Rosar María Aquino**. Que estaré toda la vida agradecida por su magnífico esfuerzo, dedicación y apoyo para seguir mi carrera y guiarme por el camino correspondiente para un gran logro hoy alcanzado, siempre me iluminaste para que hoy en día tenga esta manera de pensar tan brillante y sin duda es gracias a ti y a tu inmensa sabiduría. Todo lo que hoy en día soy es gracias a tus indicaciones y la educación que me ha llevado hasta donde hoy en día estoy, madre mía no sabes lo agradecido que estoy y a ti te dedico este maravilloso logro.

A mi padre, **Carlos Rosario Romero** por hacer un gran esfuerzo para llevarme a alcanzar todo este logro hoy en día Fue una de mi fortaleza y a él le doy las gracias por tanto esfuerzo empeñado en mi desde el inicio de la carrera hasta el final, por este y todos los logros que están por llegar, que estés presente para seguir sumando orgullos a ti que siempre has sido como un ejemplo de fuerza y valentía, gracias a ti tengo la virtud de no rendirme a la primera caída.

A mi hermana, **Karla Rossy Rosario Aquino**, eres la hermana que le vida me regalo, no tengo como agradecerte con tanto apoyo tu confianza y apoyo incondicional y por siempre ser tan empática en las situaciones que atravieso, al

momento de las peores circunstancias me reconforta saber que tengo a alguien de un nivel más cercano al mío que mis padres, me reconforte tanto como ella.

Carlos Manuel Rosario Aquino

Índice

Resumen

La presente investigación se fundamenta en el análisis de las principales técnicas para usurpación de identidad para la obtención de datos de tarjetas de crédito y débito en la República Dominicana, año 2020-2021. La suplantación de identidad con el robo de documentos e información en el ciberespacio se ha convertido en una práctica común en la Republica Dominicana, con modalidades sofisticadas y causas diversas. Dado a que estos ataques tienen alta probabilidad de éxito, combinado a la falta de información del usuario promedio y la falta de conocimiento de mecanismos de seguridad, en la Republica Dominicana es necesario establecer un enfoque centrado en la victima y los medios utilizados por los *phishers* para realizar su cometido, y así poder mitigar estos hechos. La investigación es de tipo analítica, que consiste en la desmembración de un todo, descomponiéndolo en partes o elementos para observar las causas, la naturaleza y los efectos.

Palabras clave: *Phishing, Republica Dominicana, Ingeniería Social, Ciberseguridad, Suplantación de Identidad*

Introducción

La presente investigación se fundamenta en el análisis de las principales técnicas para usurpación de identidad para la obtención de datos de tarjetas de crédito y débito en la República Dominicana, año 2020-2021. La investigación es de tipo analítica, la cual establece la comparación de variables entre distintos conjuntos de estudio y control. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías (Ortiz Frida, 2005).

En la República Dominicana se presentan diversas deficiencias en el ámbito de la seguridad cibernética, entendiendo que, estas pueden dar pie a las distintas ramas delictivas, especialmente aquellas que envuelven las sustracciones de datos personales y la suplantación de identidad, debido a que la mayor parte de la población no tienen un conocimiento “estándar” sobre el internet y la ciberseguridad. Los medios más comunes utilizados para la sustracción de datos relacionados con la identidad de una persona, para su posterior uso en la ciberdelincuencia son: Las redes sociales, ingeniería social, las confabulaciones, sorteos públicos no regulados, etc.

El estudio surge a raíz de la progresiva incertidumbre de los ciber-usuarios dominicanos, por la creciente ola de estafadores los cuales utilizan nuevas metodologías más avanzadas e ingeniería social para el robo de datos personales, tema que ha venido agravándose en los últimos años. Así como, también estudiamos los tipos de delitos cibernéticos más populares entre los *phishers* dominicanos, y consigo crear un grupo de mejores prácticas y

concientizaciones sobre el ámbito cibernético y la protección de los datos personales a los habitantes.

Se tomarán en cuenta las opciones para reducir los riesgos de suplantación de identidad al introducir datos personales altamente delicados, en este caso, más enfocado a datos bancarios.

Con este enfoque buscamos establecer patrones de control, como también tome en cuenta los resultados de este estudio para la implementación de estrategias y leyes más rígidas que permitan el desarrollo de mejores prácticas y mayores castigos para quienes infringen la ley.

Este estudio procura ser de utilidad a las partes interesadas para crear propuestas factibles para la lucha contra la suplantación de identidad. De esta manera se podrán tomar decisiones y diseñar estrategias contra este delito de acuerdo con la realidad presentada.

El análisis trae consigo una evaluación de posibles medidas que puedan ayudar a evitar o mitigar estos casos. De igual forma, aborda temas como conceptualización y particularidades de la suplantación de identidad, las metodologías utilizadas, las etapas y propósitos de la suplantación de identidad y el estudio de perfil de victimarios y victimas de suplantación de identidad.

El primer capítulo está destinado al análisis conceptualizado sobre la suplantación de identidad, conceptualizando y sobresaltando las particularidades de la suplantación de identidad, las metodologías utilizadas; cuáles son las etapas y propósitos de la suplantación de identidad, el perfil de los victimarios y víctimas de la suplantación de identidad, terminando el mismo con una pequeña conclusión parcial de este tópico.

En el segundo capítulo, se analiza la suplantación de identidad en el derecho comparado, donde se toma como guía las regulaciones de Brasil,

Colombia, Perú y España, abordando los avances en base a los controles contra este delito que estos países han tomado.

En el tercer y último capítulo, se examinan la ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, así como también el Decreto 230-18 sobre establecimiento y regulación de Estrategia Nacional de Ciberseguridad 2018-2021 y la Resolución AG/RES. 2004 (XXXIV-O/04) de la Asamblea General de la Organización de Estados Americanos (OEA), donde son contrastados con los países anteriormente abordados, en base a la realización de posibles sugerencias y soluciones para mitigar dicho delito.

Capítulo I: Análisis conceptualizado sobre la suplantación de identidad

1.1. Introducción

El presente capitulo tiene como objetivo desglosar las características y conceptos relacionados con la suplantación de identidad, conjunto a los métodos más utilizados por los ciberdelincuentes en la Republica Dominicana. En el mismo podremos observar distintas modalidades y medios los cuales estos para llevar a cabo sus actividades delictivas, por lo que es más que necesario la utilización y definición de ciertos términos técnicos para tales fines. Por otra parte, también se analizan las fases conjunto a los objetivos de estas con relación a la suplantación de identidad. Por último, desglosamos a los sujetos activos y pasivos, o, en otras palabras, el perfil de las víctimas y victimarios de esta actividad.

Antes de iniciar, es destacable un comentario realizado en un artículo para el periódico “Hoy”, compuesto por el periodista (Torres) el cual establece que: “El auge de la delincuencia cibernética y los llamados delitos electrónicos es de tal magnitud en República Dominicana que llega a mover más dinero que el narcotráfico, algo que las autoridades consideran de dimensión extraordinaria”.

Este afirma que, tomando menos riesgos y costos de operabilidad, los delitos electrónicos son más rentables y efectivos que cualquier otro delito en la actualidad. También, es necesario destacar las estadísticas que (Torres) suministra, estableciendo lo siguiente:

> El pasado año 2020 se siguieron los casos de 998 víctimas, de los cuales el 53% correspondió a mujeres. De estos casos judicializados, el 33% de los imputados fueron a prisión; 27% presentación periódica; 20% impedimento de salida del país, y 20% salió en libertad con garantía económica. Conforme los datos registrados en el primero trimestre de este año, la Fiscalía del DN

registró el ingreso de 329 casos de delincuencia cibernética, para un promedio mensual de 110 casos. Esto es una baja de 23% con relación al primer trimestre del 2020. El informe señala que el 8% de los casos trabajados tuvieron alguna decisión. De estos casos se destaca que el 24% fue declinado y el 72% archivado de manera definitiva.

El artículo de (Torres, 2021) también destacó lo siguiente: “En las estadísticas recopiladas por el departamento correspondiente de la Fiscalía del DN, sobresale el delito de alta tecnología con 43% de los 600 casos de delincuencia cibernética que fueron procesados”. Agregó: “Le siguen las estafas vía red con un 10.68%; el robo de identidad figura con un 6.18%; el chantaje recibió un 5.56%; difamación 9.02%; acceso ilícito, 3.84; clonación de tarjetas, 2.67 y la transferencia ilícita de fondos, 2.51%. Otros delitos están en sólo 2%”.

Entre las limitaciones encontradas para realizar el presente capitulo, resalta la dificultad en obtener estadísticas de entidades regulatorias (La policía Nacional y La Fiscalía del Distrito Nacional) y de los bancos de la Republica Dominicana, ya que, aunque fueron solicitadas con bastante antelación, los mismos alegan que dichos datos son confidenciales y solo de uso interno, por lo que al ser tan comprometedores no pueden ser suministrados tan fácilmente. Es destacable que, al momento de realizar las entrevistas, las dos personas entrevistadas que suministraron los datos aproximados pidieron que su participación fuese de forma anónima.

1.2. Conceptualización y particularidades de la suplantación de identidad

El *phishing* es un término otorgado a una metodología de ingeniería social1, cuya finalidad consiste en que un atacante, intenta sustraer de forma fraudulenta, credenciales y datos sensibles de usuarios legítimos, realizando copias no

[1] La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales o abran enlaces a sitios infectados.

autorizadas de datos de autenticación de medios electrónicos de servicios y organizaciones tanto públicas como privadas, así como también de redes sociales de forma automatizada. El término phishing proviene de la unión de los siguientes vocablos en inglés *password*[2], *harvesting*[3] y *fishing*, con lo que se viene a hacer alusión a "cosecha y pesca de contraseñas". A la persona que pone en práctica este delito se le conoce como "*phisher*" (Rodriguez, 2015).

Por lo general, estos realizan contacto con sus víctimas a través de correos electrónicos o llamadas, dirigiendo a su objetivo a una trampa, la cual puede ser tanto un sitio web fraudulento que recopila las credenciales de acceso, como intentar obtener los datos requeridos verbalmente.

Comúnmente las credenciales de más interés para los *phishers* en general son los usuarios/correos y contraseñas, los dígitos de las tarjetas de crédito/débito y los documentos de identificación personal. La primera mención conocida del término *phishing* se remonta a enero de 1996 en el grupo de noticias de hackers alt.2006 y fue orientado a nombrar a quienes trataban de "*pescar*" las cuentas de miembros de AOL[4] (Press, 2006).

En el *phishing* en AOL el atacante suplantaba a un empleado de AOL y enviaba mensajes instantáneos a víctimas potenciales. Para poder engañar a la victima de modo que diera información confidencial (Stutz, 1998), la metodología era hacer creer a los usuarios que se les estaba "verificando sus cuentas" o "confirmando información de factura", automáticamente el usuario suministraba su contraseña, el *phisher* accedía a la cuenta de la víctima, utilizándola para varios propósitos criminales, incluyendo la suplantación de la víctima y *spam*[5].

---

[2] Termino en ingles referente a contraseña.
[3] Termino en ingles referente a cosecha.
[4] AOL anteriormente conocida como América Online, es una empresa de servicios de internet y medios.
[5] El término SPAM o mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido.

En los últimos años se ha incrementado enormemente la tendencia a los ataques de *phishing* en la Republica Dominicana, así como la sofisticación de estos. Los datos obtenidos por esta actividad fraudulenta son utilizados para un conglomerado de actividades ilícitas las cuales van desde el fraude, el *carding*[6], y el robo con posible suplantación de identidad. Desglosando la actividad de *phishing* es destacable que este consta de 3 elementos:

- Ingeniería social: El *phisher* local busca conocer a sus víctimas en el plano personal, tratado de extraer informaciones de esta para engañarles y hacer que actúen contra sus propios intereses. Es necesario destacar que existe un grado de desconocimiento informático en la víctima del ataque al momento de utilizar el ciberespacio, cuestión que es hábilmente aprovechada por el atacante.
- Automatización: Las tecnologías de la información son usadas para llevar a cabo ataques de *phishing* de forma masiva. En cuanto a ello, una de las formas más habituales de obtención de datos para la suplantación de identidad es realizar ataques dirigido a personas al azar.
- Comunicación electrónica: Usan redes y medios sociales. Es considerable el hecho de que los medios más utilizados y efectivos para llevar a cabo estos ataques y la posterior suplantación de identidad, se realizan mediante el uso de redes y medios sociales alojados en la web.

1.3. Metodologías utilizadas

En el siguiente punto cuales son las modalidades y medios más utilizados por los *phishers* en la Republica Dominicana, para llevar a cabo la obtención de datos para la posterior suplantación de identidad de la víctima. Se explican unos cuantos conceptos y métodos relacionados con la informática y tecnología, para

[6] El Carding es el uso ilegítimo de tarjetas de crédito de otra persona.

conocer de manera detallada como se producen estos ataques. A continuación, se presentan y analizan dichos medios:

Vía mensajería instantánea: La mensajería instantánea es un medio de comunicación a través del uso de programas tipo cliente para intercambiar mensajes de texto y voz en tiempo real. Entre los programas más conocidos se encuentran: Whatsapp, Telegram, Instagram y Facebook Messenger. Estos pueden ser utilizados en diferentes aparatos con conexión a internet, como computadoras, tablets o teléfonos inteligentes. Estos, permiten el intercambio de archivos, enlaces de páginas web, imágenes y videos, lo que da pie a que los ataques por estas vías sean posibles. Sólo se necesita que la víctima haga clic en el enlace o archivo adjunto para que un código malicioso se ejecute sin intervención del usuario. Es necesario destacar que hay un trabajo previo del *phisher* al momento de elaborar el mensaje malicioso. En estos casos, diversos autores expertos en ciberseguridad recomiendan que el usuario verifique la procedencia y contenido de la mensajería que llega a su dispositivo y que incluso ante la duda, no ejecute ningún tipo de operación, evitando así el dominio y la extracción de información confidencial de parte del hacker, mucho más si no conoce a la persona que le envía dicho mensaje.

Vía Email: Los *phishers* pueden enviar millones de emails a listados de posibles víctimas creado por el atacante o compradas a organizaciones dedicadas a este fin. Estos e-mails son característicos por sus títulos inusuales que hacen anuencia a algún tipo de urgencia; esto sirve para captar la atención de la víctima y lograr que realice las peticiones que demande el correo electrónico. Los *phishers* se aprovechan de las fallas de diseño dado a que manejan texto plano, así el atacante envía e-mails engañosos, agregando al cuerpo del mensaje un enlace con semejanza al nombre de la página legítima o archivos adjuntos con código malicioso, por lo qué; si el usuario no se detiene a leer con cuidado el mensaje recibido, puede ser víctima del ataque.

Spear Phishing: El *spear phishing* es un fraude de suplantación de identidad vía email. La gran diferencia de este con los ataques de *phishing* común es que mientras el *phishing* común envía mensajes aleatorios a un conglomerado de posibles víctimas, el *spear phishing* está dirigido a una organización o persona en particular.

Los ataques de *spear phishing* tienen altas probabilidades de ser exitosos porque no son detectados fácilmente por herramientas de antispam. La secuencia del ataque consiste en 4 pasos:

- Primero El atacante ubica la información de contacto de la persona u organización a atacar.
- Segundo, se detecta, un acceso a un sistema de su interés que requiere autenticación con usuario y contraseña.
- Tercero, busca datos de contacto que aparecen en la página web de la organización para crear un correo electrónico que parezca auténtico, utilizando la identidad de un individuo autorizado para solicitar información confidencial.
- Cuarto, envía el email a una persona particular o algún empleado de la organización a atacar, solicitando información sensible o indicarle que se autentique

Vía Whaling: Se puede decir, que la técnica de *whaling* es parecido a *spear phishing*, solo que más avanzada ya que, aunque se basen en el mismo concepto, este solo ataca a personas de altos cargos ejecutivos y líderes claves dentro de importantes corporaciones empresariales y políticas. El *whaling* no es un *spam*; ya que requiere de la investigación previa a un alto ejecutivo determinado, para así elaborar un e-mail personalizado, que sea lo más genuino y legitimo posible.

En la investigación preparativa de esta rama del *phishing*, se buscan elementos puntuales como título profesional, correo electrónico personal y laboral,

números telefónicos y nombres de personas de jerarquía similar en la corporación. El objetivo principal del *phisher* o hacker en este hecho es obtener el control parcial o total de la computadora de la víctima para conseguir información relevante. Es necesario considerar que, dado a la alta sofisticación de este método, las corporaciones deben contar con personal capacitado que pueda verificar estos correos en un ambiente controlado y es necesario la implementación de software de seguridad informática.

Vía Páginas Web: Estos ocurren cuando la víctima accede a un sitio web no seguro el cual tiene una inserción de código malicioso o explotando una vulnerabilidad existente en el servidor web, aplicación o browser del usuario, como puede ser el redireccionamiento de un enlace a un sitio malicioso. El *phisher* puede crear una página pirata con un nombre de dominio semejante a uno fidedigno, para luego ejecutar el código malicioso desde ahí.

Un ataque de phishing puede ser realizado a través de una página web y puede ir desde la creación de publicidad falsa en internet, banner, con texto y/o imágenes gráficas para redirigir al usuario a su página web y obtener información personal y confidencial; asimismo, se utilizan ventanas emergentes conocidas como pop-up, simulando provenir de un sitio válido, que anuncia diversas amenidades, y pueden redirigir a una página web falsa.

Es frecuente a su vez que los *phishers* saquen ventaja de una vulnerabilidad conocida en un browser, insertándole contenido malicioso, por ejemplo, *keyloggers*[7], captura de pantalla, *backdoor* (puertas traseras), troyanos[8],

[7] Los *keyloggers* realizan un seguimiento y registran cada tecla que se pulsa en una computadora, generalmente sin el conocimiento del usuario

[8] Un troyano es un tipo de programa maligno que a menudo se camufla como software legítimo.

botnet[9] y otros programas, desde una página web oficial previamente comprometida para descargarlo a la computadora de la víctima.

Por último, los *phishers* se aprovechan del exceso de confianza que tienen los usuarios para almacenar claves, cookies e historial en el navegador, como asimismo explotan alguna vulnerabilidad del navegador de la víctima o protocolo que la afecte.

Vía Vishing: El ataque de *phishing* basado en voz sobre IP es denominado vishing. Por lo general, estos ciberdelincuentes pueden llamar a un directorio de números telefónicos de una región o tener acceso a una lista de teléfonos de una organización o de personas.

En una llamada telefónica se tiene interacción humana entre la víctima y el victimario para persuadir a la persona de otorgar datos como fecha de nacimiento, fecha de expiración de tarjetas, PIN, entre otros. El *phisher* se hace pasar por una entidad de confianza, indicando que hubo algún tipo de problema, por ejemplo: necesidad de cambiar el PIN de tarjeta o autorizar un pago.

Si bien todas las personas se encuentran expuestas a este tipo de ataques, los objetivos más vulnerables frecuentemente son las personas de la tercera edad, quienes, en su gran mayoría, no se imaginan que están siendo víctimas de *phishers*, por lo que proporcionan todos los datos que le son solicitados.

Vía Sim Swapping: El *SIM Swapping* es un fraude realizado mediante la tarjeta SIM. Este permite acceder a cuentas ajenas mediante la explotación de una debilidad en la autenticación de múltiples factores en la que el segundo factor es un mensaje de texto (SMS) o una llamada realizada a un teléfono móvil.

[9] Una *botnet* es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido

El fraude explota la capacidad de un proveedor de servicios de telefonía móvil para transferir un número de teléfono a un dispositivo que contiene una tarjeta SIM[10] diferente. Esta función se usa normalmente cuando un cliente ha perdido o le han robado su teléfono.

La estafa comienza con un *phisher* que recopila datos personales sobre la víctima, ya sea mediante el uso de correos electrónicos de *phishing*, comprándolos a ciberdelincuentes o directamente manipulando a la víctima.

Una vez que el *phisher* tiene estos datos, se pone en contacto con el proveedor de telefonía móvil de la víctima. Este utiliza técnicas de ingeniería social para convencer a la compañía telefónica de que transfiera el número de teléfono de la víctima a la SIM del estafador. Esto se hace, haciéndose pasar por la víctima utilizando los datos personales de la misma, y alegando que se le ha perdido o le han robado su teléfono. En la Republica Dominicana, el defraudador tendrá que convencer directamente al empleado de la empresa de telecomunicaciones, los cuales son sobornados para llevar a cabo el proceso de traspaso de la SIM.

Por otro lado, es necesario destacar, que también existe la posibilidad de realizar dicha práctica con los vendedores ambulantes de SIM, los cuales también son convencidos de igual forma, para que estos les suministren una SIM a nombre de otra persona de la cual estos puedan información robada.

Una vez que esto suceda, el teléfono de la víctima perderá la conexión a la red y el estafador recibirá todos los SMS y las llamadas de voz destinadas a la víctima. Esto le permite al estafador interceptar cualquier contraseña de un solo uso enviada a través de mensajes de texto o llamadas telefónicas enviadas a la víctima, y así eludir cualquier característica de seguridad de las cuentas (ya sean

[10] Una SIM es una tarjeta inteligente que almacena la clave de servicio del suscriptor utilizada para identificarse ante la red.

cuentas bancarias, cuentas de redes sociales, etc.) que dependen de mensajes de texto o llamadas telefónicas.

1.4. Etapas y propósitos de la suplantación de identidad

El análisis de las fases o etapas puede ser de gran utilidad para combatir a los *phishers*. En ocasiones estas pueden variar dependiendo del nivel de estafa debido a la existencia de diferentes variantes de fraude, al igual que todo lo respectivo a extensión, dificultad, personas que deben intervenir y papeles a desempeñar.

Fase 1: El estudio

La primera decisión tomada por el victimario en esta fase es qué tipo de datos desea conseguir, cómo puede ser información de cuentas bancarias, nombres de usuario y contraseñas o datos personales de diversa índole. Esta cuestión estará vinculada a cuál es el tipo de engaño que se intenta cometer. Asimismo, es de suma importancia poder determinar la institución o empresa a suplantar, ya que muchas de las estafas implican que el *phisher* suplante la identidad de un agente de una entidad en la que la víctima tenga confianza. Esta es la primera fase previa para llevar a cabo la planeación y realización del ataque, por lo que el *phisher* se encarga de realizar un análisis íntegro de la o las personas u organizaciones que pretende atacar y recopilar información que le sea de utilidad, y así saber cómo llevar a cabo el delito.

Fase 2: La planificación

Durante esta etapa, el *phisher* se encarga de tomar las principales decisiones de cómo se llevará a cabo el hecho. Aquí el *phisher* decide cómo y dónde se va a realizar, o qué medios necesitará para hacerlo y qué tipo de falacia utilizaran. Una de las cuestiones que se plantea un *phisher* en esta fase, cualquiera que sea la modalidad elegida, es la decisión de realizar el ataque de

forma conjunta o individual. La planificación es variable y puede consistir desde la aceptación de una base de direcciones electrónicas conseguidas al azar, hasta el *spear phishing*, que puede conllevar el estudio detallado del perfil de las víctimas, pasando por las posibilidades existentes entre ambos extremos.

Fase 3: La preparación

Algunas de las tareas que deben realizar los delincuentes es conseguir el software, los datos de contacto, localizar los destinos de sus ataques, preparar sus equipos, construir los sitios web diseñados para efectuar el fraude y otras tareas, teniendo en cuenta las necesidades de cada tipo de modalidad. En ocasiones, los *phishers* realizan ataques dirigidos a personas u organizaciones específicas, lo que requiere el envío de correos mucho más sofisticados que los que se utilizan en envíos masivos.

Fase 4: El ataque

Aquí se realiza el robo de datos o de identidad como tal. Esta etapa es particular debido a que implica la colaboración de la víctima a realizar diversas acciones como abrir un correo electrónico, visitar una página web, realizar una búsqueda, o sencillamente a suministrar una o un conjunto de informaciones. En cuanto a las tareas, no hay un patrón establecido, debido a que todo va a depender del tipo de *phishing* seleccionado. Es necesario constatar que, en esta fase, toda la planificación y preparación realizada por los hackers informáticos necesita de la “colaboración” o “interacción” de la o las persona u organizaciones a las que van.

Fase 5: La recolección de datos

La fase de recolección de datos implica actividades de “colaboración” de la víctima como se mencionó anteriormente. Esto está sujeto directamente a la espera de que las víctimas interactúen en el servidor atacado, que respondan al

mensaje enviado o que visiten la web fraudulenta. Claro está que no en todos los casos la suplantación de identidad tendrá resultados positivos para los *phishers*, aunque son presa fácil aquellos individuos que no tiene conocimientos en informática, y que a su vez realizan actividades sin precaución del caso ni el asesoramiento adecuado.

Fase 6: La ejecución del fraude

Culminada la recolección de los datos de la víctima, el *phisher* realiza del fraude, que puede ser directo o indirecto (Venta de los datos obtenidos para que otros estafadores lleven a cabo este tipo de modalidad). Aunque la suplantación de identidad en estos casos solo es abordada con fines de hurtar a través de la información confidencial recabada, también es necesario destacar que en otros casos también puede tener como finalidad el daño a la imagen.

Fase 7: La eliminación de rastros

La última fase, está referida a la necesidad que tienen los *phishers* de eliminar todas aquellas pistas o rastros que hayan quedado del ataque efectuado, y que pueda conducir al autor o autores intelectuales. Es necesario destacar que, los estafadores procederán luego al blanqueo de los beneficios obtenidos de la operación.

1.5. Perfil de victimarios y victimas de suplantación de identidad

Victimarios:

En la Republica Dominicana existen varios tipos de ciberdelincuentes que realizan estas acciones, en los cuales se pueden identificar dos grandes grupos:

Aquellos delincuentes que actúan solos, generalmente de una franja de menores de 25 años y con conocimientos técnicos limitados pero que sirven a sus objetivos.

Grupos organizados, compuestos por personas con distintas especialidades y recompensas de acuerdo con sus funciones del riesgo que asumen dentro del grupo.

Es necesario destacar un estudio realizado por (Abad.), que involucró el monitoreo de salas de chat en las que habitaban los *phishers*, resume que el *phishing* por lo general es realizado en asociaciones de malhechores, lo que permite que diferentes piratas informáticos, *phishers* y *spammers* realicen sus ataques. Abad descubrió que había varias categorías de especialización laboral, como remitentes, recolectores y cambiadores, los cuales nos van a ayudar a desglosar a los mismos como se define a continuación:

Los ***remitentes*** son spammers o piratas informáticos que tienen la capacidad de enviar una gran cantidad de correos electrónicos fraudulentos. Esto generalmente se hace a través de redes de bots.

Los ***recopiladores*** son piratas informáticos que han creado sitios web fraudulentos a los que el *spam* fraudulento dirige a los usuarios y que solicitan activamente a los usuarios que proporcionen información confidencial, como nombres de usuario, contraseñas y números de tarjetas de crédito. Estos sitios web generalmente están alojados en máquinas comprometidas en Internet.

Los ***cashers*** toman la información confidencial recopilada por los recolectores y la utilizan para lograr un pago. Esto se puede hacer de varias maneras, desde la creación de tarjetas de crédito y tarjetas bancarias fraudulentas que se utilizan para retirar dinero directamente de los cajeros automáticos hasta la compra y venta de bienes. Se sabe que los recaudadores pagan a los recaudadores directamente por la información personal correspondiente a los usuarios o cobran comisiones, donde reciben un cierto porcentaje de los fondos que eventualmente se recuperan de la información.

Victimas:

La víctima del ilícito es el ciber-usuario sin ningún conocimiento técnico, siendo uno de los sujetos pasivos más vulnerables y expuestos a los distintos ataques de suplantación de identidad. También es necesario destacar que las entidades comerciales, financieras y crediticias conceden servicios, créditos y entrega de fondos a terceros no apropiadamente identificados, o que realizan controles débiles y fácilmente evitables por los delincuentes.

Finalmente, el Estado que ante su actuar negligente, también lo transforma en parte responsable, porque posibilita la comisión del ilícito a través de la falta de normativa, campañas de concientización y controles indispensables a la documentación del ciudadano, la dificultad para denunciar esta actividad ilícita.

1.6. Conclusiones parciales

Entendemos que, luego de la exposición técnica sobre estos medios empleados, más allá que es de suma importancia el conocimiento, capacitación y aprendizaje sobre la temática abordada, lo determinante es poder detectar y prevenir eficazmente la presencia de algún hacker o *phisher* que esté intentando acceder a la información confidencial del usuario para repeler las potenciales consecuencias perjudiciales de este tipo de ataque. Lo crucial del asunto está orientado a la tarea de detección y prevención por partes de los usuarios para no ser presa fácil de estos suplantadores, ya que una vez que logran ingresar a los datos personales del individuo, pasan a tomar el dominio de la situación que en muchos casos es irreversible.

Capitulo II: Análisis de la Suplantación de Identidad en el derecho comparado

1.7. Introducción

En este segundo capítulo se hará un análisis comparativo entre los países de Latinoamérica, Brasil, Perú y Colombia, se tomara como referencia de investigación de Europa a España, esto para mostrar cual es el estado que se tiene contra una de las potencias mundiales en habla hispana, esto en el ámbito de las leyes que penalizan o tratan de penalizar la suplantación de identidad cuyo fin será estudiado, en conjunto con el tratamiento, la regulación jurídica y el código penal de los países que estarán articulados más adelante.

1.8. Regulación Brasileña

En el país brasileño, fue sancionada en el año 2012 la ley 13.737 de delitos informáticos, cambiando el código penal de Brasil en los artículos 154-A y 154-B dentro de la sección IV: “de los crímenes contra la inviolabilidad de los secretos”.

En el análisis a realizar en este país, no existe una ley que explícitamente sancione el acto de suplantación de identidad, solo existe la regulación mediante los 2 artículos antes mencionados.

En el Articulo 154-A. este hace referencia a la injerencia realizada en un equipo informático sin autorización expresa o tácita, las penas que castigan esta conducta delictiva van en aumento dependiendo el tipo de daño a la persona afectada, este dice que:

> “Invadir el dispositivo informático ajeno, conectado o no a la red de ordenadores, mediante infracción indebida de un mecanismo de

seguridad y con el fin de obtener, adulterar o destruir datos o informaciones sin autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades para obtener ventaja ilícita: pena - detención, de 3 (tres) meses a 1 (un) año, y multa".

1º. En la misma pena incurre quien produce, ofrece, distribuye, vende o difunde dispositivo o programa de ordenador con el fin de permitir la práctica de la conducta definida en el encabezado.

2º. Se aumenta la pena de un sexto a un tercio si de la invasión resulta perjuicio económico.

3º. Si de la invasión resulta la obtención de contenido de comunicaciones electrónicas privadas, secretos comerciales o industriales, informaciones sigilosas, así definidas en ley, o el control remoto no autorizado del dispositivo invadido: pena - reclusión, de 6 (seis) meses a 2 (dos) años, y multa, si la conducta no constituye un crimen más grave.

4º En la hipótesis del inc. 3º, se aumentará la pena de uno a dos tercios si hay divulgación, comercialización o transmisión a tercero, a cualquier título, de los datos o informaciones obtenidos.

5º Se incrementa la pena de un tercio a la mitad si el crimen se practica contra:

I - presidente de la República, gobernadores y alcaldes;

II - presidente del Supremo Tribunal Federal;

> III - presidente de la Cámara de Diputados, del Senado Federal, de Asamblea Legislativa de Estado, de la Cámara Legislativa del Distrito Federal o del Ayuntamiento;
>
> IV - Dirigente máximo de la administración directa e indirecta federal, estadual, municipal o del Distrito Federal.

En cuanto al art. 154–B, menciona la acción penal referida al art. 154–A, rezando:

> En los crímenes definidos en el art. 154–A no sólo se realiza mediante representación, salvo si el delito se comete contra la administración pública directa o indirecta de cualquiera de los Poderes de la Unión, Estados, Distrito Federal o Municipios o contra empresas concesionarias de servicios públicos.

1.9. Regulación Colombiana

La suplantación de identidad se encuentra regulada en el país colombiano mediante el título VII bis: “de la protección de la información y de los datos” del código penal colombiano, en un artículo en específico el articulo 269G: “suplantación de sitios web para capturar datos personales”, que reza:

> El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

También indica que:

> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito. Este describe en conjunto con la estafa la importancia del https (sitio seguro), en el internet tanto individual como empresarial. El articulo describe lo que comúnmente se conoce como *phishing*.

Un punto para tomar en consideración es que en el mismo artículo en el apartado H, del código, agrega circunstancias de conductas punitivas de las penas del articulo descrito anteriormente, esta cita:

> Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
>
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
>
> 2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

1.10. Regulación Peruana

La suplantación de identidad en Perú, esta penalizada de manera regular y genérica mediante la sanción de la ley 30096 de delitos informáticos, promulgada en el año 2013 por el congreso peruano en el artículo 9 que complementa el código penal de este país, complementando las sanciones de los delitos informáticos que atenten a la fe pública. Este articulo expresa:

Art. 9. Suplantación de identidad. El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio,

material o moral, será reprimido con pena privativa de la libertad no menor de tres ni mayor de cinco años.

Este articulo menciona que, el hecho debe estar encasillado en la descripción del artículo, por otro lado, también se menciona la pena a la que esta supuesta el crimen.

1.11. Regulación Española

En el país español, el tema jurídico de los delitos informáticos tiene 2 partes: Están los que explican de manea clara que los delitos cibernéticos no existen, ya que se reduce al hecho de ser cometido en un equipo informático. Por lo tanto, no sería necesario una ley para este. La contraparte sostiene que deben separarse estos delitos de los tradicionales o tener un tratamiento diferente, o la decisión de la regulación conjunta.

La ley española en su código penal no contiene un artículo propio a los delitos cibernéticos, estando su definición en los correspondientes delitos tradicionales. Lo que se denomina como "*phishing*", está incluido de forma común, en el código penal español, en el capítulo VI: "de las defraudaciones, sección 1ª de las estafas, dentro de los delitos de naturaleza económica que afectan patrimonialmente a la persona".

En este grupo, el crimen más común es la estafa informática. Normalizado en el artículo 248 del código, en el inciso 1, se clasifican las estafas basadas en las técnicas de ingeniería social pura (donde está el *phishing*), citando que: "cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno"; y los supuestos de utilización de código malicioso (malware) o de intrusión en sistemas de información son recogidos en el art. 248 inciso 2º a) del

Código Penal Español, el que reza “también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero”.

El congresista contempla la posibilidad de crimen en grado de la tentativa en el 3er apartado del artículo, por lo que la compra, posesión o distribución de virus (Malware, Ramsonware, Day Zero), puede considerarse un delito.

1.12. Conclusiones parciales

Ya analizado y estudiado la suplantación de identidad en los países mencionados más arriba, dejamos en claro que no en todas existen las legislaciones para sancionar estas prácticas. En casos como Brasil y España, vemos que no existe un tipo penal específico sobre la suplantación de persona, sin importar los casos que este conlleve dentro.

Por esta razón debe de haber una reforma en la que se incluya la suplantación de identidad como delito, con determinación de tiempo en cárcel. En Colombia, República Dominicana y Perú está a la vista el avance que se ha efectuado en contra de esta técnica, ya que establecen en su ley, definida ya, que dependiendo el tipo de caso la pena es variable.

Capitulo III: Marco Regulatorio de la Suplantación de Identidad en la Republica Dominicana

1.13. Introducción

En la República Dominicana no se han establecido controles de seguridad efectivos, que eviten la sustracción de información personal. Esto, dado a la falta de una ley más robusta en este ámbito (Ley de suplantación de identidad), y mejor preparación de los estamentos del estado que tienen la tarea de resolver dichos casos y evitar/mitigar posibles casos a futuro.

Cuando hablamos de derecho civil, cabe aclarar, que nos estamos refiriendo a un conjunto de normas legales y de principios de derechos que regulan las relaciones entre las personas y los patrimonios, entre personas públicas y también personas privadas.

En el concepto inicial, debemos aclarar todos los análisis, que se encuentra ya los elementos que suscitan la necesidad de una investigación minuciosa, y por los tantos constituyentes desde el punto de partida hasta el punto final. El derecho civil se muestra como una de muchas ramas importante y más fundamentales para el sostén del aparato jurídico de todas las naciones. Así como todo país organizado deben de tener leyes.

1.14. Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología

En la Republica dominicana, en el año 2007 se promulga la ley 53-07contra crímenes y delitos de alta tecnología, donde en el artículo 17 de dicha ley se hace referencia a la amonestación y a la pena mínima y/o máxima a la que se puede condenar a un imputado por robo de identidad citando este articulo:

> Artículo 17.- Robo de Identidad. El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo.

Este expresa lo que es, la pena mínima, máxima y la multa que puede contraer el criminal.

En la actualidad el conocimiento la información y los instrumentos informáticos de comunicación son cada vez más importantes y trascedente en todos los procesos de desarrollo competitivo registrados en la vertiente económica, social, empresarial, política. Los principios generales de esta ley son:

Principio de Territorialidad: Esta ley penal se aplica a delitos cometidos en el territorio de la República Dominicana. Sin embargo, las infracciones del artículo constituyen un atentado al territorio nacional, ya que los delitos o faltas previstos en esta ley se cometen fuera del territorio de la República del en las condiciones previstas en los incisos b y c, quedando el sujeto activo, en caso de que no haya sido juzgado mediante sentencia definitiva por el mismo hecho o evadido la persecución penal en tribunales extranjeros, a la disposición de la jurisdicción nacional.

Principio de Razonabilidad y Proporcionalidad: Las restricciones y prohibiciones deben ser proporcionales al propósito y los medios de peligro que intentan evitar, y el impacto social de la decisión debe considerarse cuidadosamente. Al aplicar las sanciones impuestas por esta ley, los jueces

competentes toman en cuenta la gravedad de los hechos cometidos, y las sanciones se aplican no solo a las personas a quienes se aplica el, sino a la sociedad en su conjunto. un impacto social y reproducible.

1.15. Decreto 230-18 sobre establecimiento y regulación de Estrategia Nacional de Ciberseguridad 2018-2021

Tomando en cuenta este decreto nos habla de la republica dominicana como estado social y democrático de derecho organizado en forma unitaria siempre poniendo en alto el respeto humano de los derechos fundamentales.

El objetivo de este decreto es regular y establecer las estrategias nacionales de ciberseguridad en los, así como los mecanismos de ciberseguridad para la protección del estado sus personas físicas y desarrollar la seguridad nacional

El marco de acción de este decreto contempla:

- Alianzas nacionales
- Marco legal y fortalecimiento institucional
- Educación
- Cultura nacional

El objetivo general de este es fortalecer el marco legal que incluye los temas con la ciberseguridad. Es destacable que este indica en su línea de acción 1.1 que debe establecerse un plan de actualización y reforma detallada del marco jurídico vigente, el cual es la ley 53-07. También en la línea de acción fomenta a

fortalecer la relación del servicio de la Policía Nacional con el público, para fomentar la confianza para la notificación de delitos cibernéticos.

En el Articulo 7. Pilar 3, denominado “Educación y Cultura Nacional de Ciberseguridad” tiene como objetivo fomentar la capacitación en ciberseguridad en todos los niveles del sistema educativo e impulsar una cultura nacional de ciberseguridad, donde se hablen de los conceptos fundamentales del mismo. Así como establece también el objetivo especifico 4, que es sensibilizar a la sociedad civil y política en los temas de ciberseguridad y el uso responsable de las tecnologías de información.

1.16. Resolución AG/RES. 2004 (XXXIV-O/04) de la Asamblea General de la Organización de Estados Americanos (OEA)

Considera que las resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas sobre la lucha contra la utilización de la tecnología de la información para fines delictivos, la resolución 57/239 relativa a la creación de una cultura mundial de seguridad cibernética y la resolución 58/199 sobre creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales; y Que en su XII Reunión, el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (COM/CITEL) señaló que “la creación de una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones aumentando la conciencia entre todos los participantes de las Américas en las redes y sistemas de información relacionados con el riesgo de dichos sistemas y desarrollando las medidas necesarias para hacer frente a los riesgos de seguridad respondiendo rápidamente a los ciber-incidentes” es parte de los mandatos impartidos por el CITEL.

1.17. Conclusiones parciales

Luego de revisar y analizar la situación en el marco legal de la Republica Dominicana en el ámbito de ciberseguridad, comparado con las leyes internacionales, encontramos deficiencia en la misma, ya que apenas existe un solo artículo que hable sobre el robo de identidad, dejando fuera demás delitos que puedan ser realizados al momento de la suplantación de identidad, como lo es la sustracción de los datos bancarios de la víctima para el posterior uso. Es claro que el decreto 230-18 conlleve a la modernización y adecuación de esta ley, tomando como parte de su iniciativa la formación de la población en torno a este ámbito, así como también es necesario la creación de leyes que sean más rígidas para poder atender dichos casos, los cuales, vistas las estadísticas anteriormente mencionadas, terminan archivados.

En resumen, la ley debe ser más punitiva, ya que el artículo de la ley 53-07 es muy genérico y sin importar el crimen o la gravedad de este la pena sigue siendo igual que otro que sea de menor categoría.

Conclusiones

En el presente trabajo, concluimos que la suplantación de identidad, o phishing es el termino otorgado al conjunto de prácticas, que tienen como fin sustraer de forma fraudulenta y, sobre todo, no autorizada, de datos y credenciales de autenticación en medios electrónicos de personas, para posteriormente utilizarlos en su beneficio, y en perjurio de la víctima del fraude. Particularmente los *Phishers* dominicanos suelen contactar sus víctimas a través de correos electrónicos o llamadas, buscando así que la persona a las que estos intentan engañar acceda a sus cuentas de redes sociales o bancos, mediante páginas web fraudulentas las cuales se asemejan a paginas de sitios seguros, con el fin de obtener los datos de la persona. También se dan los casos de que estos "confirman" las informaciones personales de las victimas con los mismos por teléfono, que por lo general obtienen de esta práctica, del soborno o confabulación con alguna persona que trabaje dentro de empresas que acceda a datos de posibles víctimas, o que datos que compran en el mercado negro.

En los últimos años en la Republica Dominicana es notable un incremento de la tendencia a ataques de phishing, así como el nivel de sofisticación y de detalles que estos toman en cuenta. Es destacable que, de este delito, pueden surgir otros, los cuales pueden ir desde el carding, el chantaje y el daño de imagen de una persona.

El phishing o usurpación de identidad consta de 3 elementos claves para la ejecución de este: La ingeniería social que consiste en recopilar todos los datos posibles de la víctima; la automatización, que consiste en utilizar tecnologías de información para llevar a cabo los ataques; y por último la comunicación electrónica, que consta en la utilización de redes y medios sociales para llevar a cabo el delito.

Entre las metodologías más utilizadas destacamos la utilización de mensajería instantánea, el envío de *spam* a través de e-mail; el *Spear* phishing que envía un mensaje a una organización o persona en particular; el Whaling que está basado en el *Spear* phishing, con la diferencia de que este solo ataca a altos ejecutivos y políticos; el uso de paginas web, de las cuales se aprovechan de las vulnerabilidades de las mismas; Vía Tabnabbing donde solicitan a los usuarios las credenciales de acceso a sus cuentas de correo o redes sociales; Via Vishing que son las llamadas falsas; y por ultimo pero no menos importante, el SIM Swapping que es cuando estos sacan chips a nombre de otras personas.

Dado a lo estudiado, pudimos establecer que existen 7 etapas para la suplantación de identidad, que son: El estudio, la planificación, la preparación, el ataque, la recolección de datos, la ejecución del fraude y la fase de eliminación de los rastros. En el estudio el *phisher* establece su objetivo a conseguir. En la planificación toma las principales decisiones de como llevara el hecho a cabo. En la preparación reúne los elementos a utilizar para llevar a cabo el hecho. En el ataque es cuando realiza el robo de datos o de identidad como tal. En la recolección de datos como su nombre lo indica, recopila todo lo conseguido. En la ejecución de fraude este vende o utiliza los datos recopilados para el posterior robo de fondos. Por último, es la eliminación de rastros que es donde este trata de no dejar nada que dé con el mismo.

En la Republica Dominicana existen diferentes tipos de *phishers* que realizan estas acciones, los cuales son divisibles en 2 grupos: Aquellos menores de 25 años y con conocimientos técnicos limitados que sirven a sus objetivos, y los grupos organizados, compuestos por personas de distintas ramas del phishing. También observamos que, estadísticamente hablando, solo en el 2020 la Fiscalía del Distrito Nacional recibió 998 casos donde el 53% de los afectados eran féminas. Según los datos que expone el periodista (Torres), en el primer trimestre del año 2021 se han registrado 329 casos de delincuencia cibernética, el

equivalente a 3 casos diarios, y para un promedio mensual de 110 casos. Aunque es una baja del 23% relacionado al primer trimestre del año 2020, el mismo afirma que solo el 8% de los casos, o exactamente 26 casos han tenido alguna decisión, el 24% equivalente 72 casos fueron declinados y el 72% equivalente a 237 fueron archivados de manera definitiva. Estos realizaron una estimación de 600 casos hasta junio, donde se arrojaron los siguientes resultados aproximados de denuncias que han recibido: 253 casos de delitos de alta tecnología, 64 casos de estafas vía red, 40 casos de robo de identidad, 23 casos de acceso ilícito, 15 casos de transferencia ilícitas de fondos, la clonación de tarjetas 16 casos, y por último 189 entre otros delitos.

Esto deja constar que existe una brecha educacional de la población dominicana, la cual es aprovechada por los *Phishers* para así proceder al robo de sus credenciales, las cuales generalmente son tarjetas de crédito y debito para su posterior venta o uso personal.

Por último, pudimos observar las leyes de Brasil, Colombia, Perú y España, donde pudimos concluir que, a pesar de no existir la ley contra la usurpación de identidad, si penalizan las actividades relacionadas al phishing como tal, a diferencia de la Republica Dominicana, que como bien ya se ha mencionado en el capitulo 3, solo tenemos en la ley 53-07 el articulo 17 el cual penaliza el robo de identidad, por lo que surge el decreto 230-18 sobre establecimiento y regulación de estrategia nacional de ciberseguridad 2018-2021 tomando en cuenta también la resolución AG/RES. 2004 (XXXIV-O/04) de la Asamblea General de la Organización de Estados Americanos (OEA). El decreto 230-18 entre sus particularidades establece como objetivo la concientización a la población civil, cosa la cual no ha pasado como se pudo dejar contrastado en la encuesta que hemos realizado, donde los participantes están de acuerdo en relación con una campaña sobre el tema, y la modernización sobre el ámbito

regulatorio para que los casos de estos robos puedan ser procesados con mayor rigor.

Recomendaciones

Para evitar la usurpación de identidad, podemos citar varias recomendaciones las cuales son mencionadas a continuación:

- Es necesario contar con contraseñas robustas para las cuentas utilizadas.
- Utilizar autenticación en 2 pasos.
- Solo utilizar paginas seguras, las cuales cuenten con certificados de confianza.
- Leer los correos atentamente.
- No abrir enlaces de correos no conocidos.
- No participar en sorteos que no sean regulados, esto debido a que cuando son culminados, no hay certeza de cómo son destruidos los datos que se introducen en los boletos.
- Pedir ayuda a expertos.
- No brindar informaciones personales por teléfono.
- Comunicarse con un representante de banco en caso de recibir un correo de este.

En el caso del Estado, es necesario la creación de campañas de concientización, ya que es de más mencionar que estas se hacen, pero con la salvedad de que son solo a nivel interno de las instituciones; es necesario crear conciencia sobre el tema entre los usuarios menos conocedores para que no caigan en dichos engaños. También es destacable la necesidad de reestructuración de la ley 53-07, dado a los avances de los tiempos y consigo la sofisticación de las técnicas y medios de los ciberdelincuentes para llevar a cabo sus actos.

Referencias Bibliográficas:

- Abad., C. (2005, 9 9). *The economy of phishing: A survey of the operations of the phishing market.* Obtenido de First Monday: https://firstmonday.org/ojs/index.php/fm/article/view/1272/1192
- Bishop, M. (2003). ¿What is Computer security? *IEEE Security and Privacy Magazine*, 67-69.
- Markus Jakobsson, S. M. (2007). *Phishing and Countermeasures.* New Jersey: John Wiley y Sons, Inc.
- Ortiz Frida, G. M. (2005). *Metodologia de la investigacion.* Mexico : Editorial Limusa.
- Press, O. U. (2006, 8 9). *Oxford English Dictionary Online*. Obtenido de http://dictionary.oed.com/cgi/entry/30004303/
- Rodriguez, M. V. (2015, 10 30). *Noticias Juridicas*. Obtenido de Estafa informática. El denominado phishing y la conducta del 'mulero bancario': categorización y doctrina de la Sala Segunda del Tribunal Supremo: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/
- Stepp, E. (1993). *The virtualisation of institutes of research.* Electronic journal of virtual culture.
- Stutz, M. (1998, 1 29). *AOL: A Cracker's Paradise?* . Obtenido de https://web.archive.org/web/20051222120913/http://wired-vig.wired.com/news/technology/0,1282,9932,00.html
- Torres, J. A. (2021, 5 21). Delitos electrónicos RD mueven más dinero que el narcotráfico. Santo Domingo, Distrito Nacional, Republica Dominicana.

- Zunzunegui, S. (2008). El ciberterrorismo, una perspectiva legal y judicial. *Cuaderno del Instituto Vasco de Criminología*, 171.

Legislación:

A) Legislación Internacional:

1. Ley de delitos informáticos de Brasil Número 12.377: Artículos 154-A y 154-B del Código Penal de Brasil.
2. Código Penal de Colombia. Arts. 269-G y 269-H.
3. Ley de delitos informáticos de Perú, número 30.096: Artículo 9 del Código Penal de Perú.
4. Código Penal de España. Art. 248 incisos 1 y 2.
5. Resolución AG/RES. 2004 (XXXIV-O/04) de la Asamblea General de la Organización de Estados Americanos (OEA)

B) Legislación Nacional:

1. Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología: Articulo 17 - sobre el robo de identidad.

2. Decreto 230-18 sobre establecimiento y regulación de Estrategia Nacional de Ciberseguridad 2018-2021

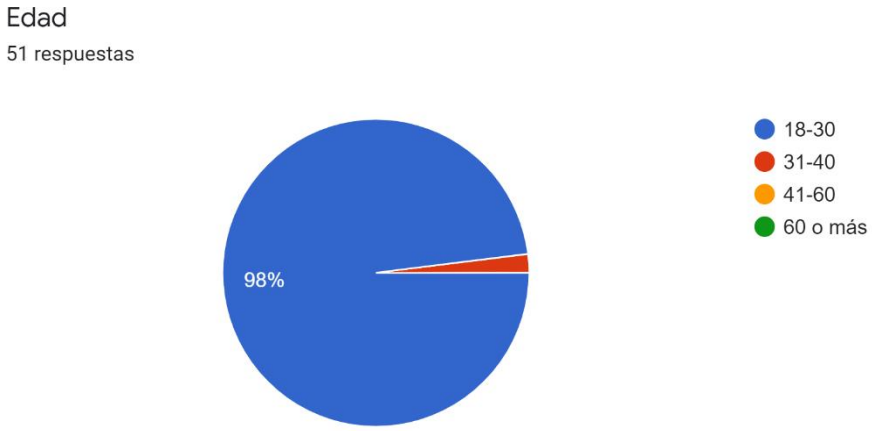
Anexos

Anexo 1. Encuesta realizada al público.

1. Edad:

A. 18-30 = 50
B. 31-40 = 1
C. 41-60 = 0
D. 60 o más = 0

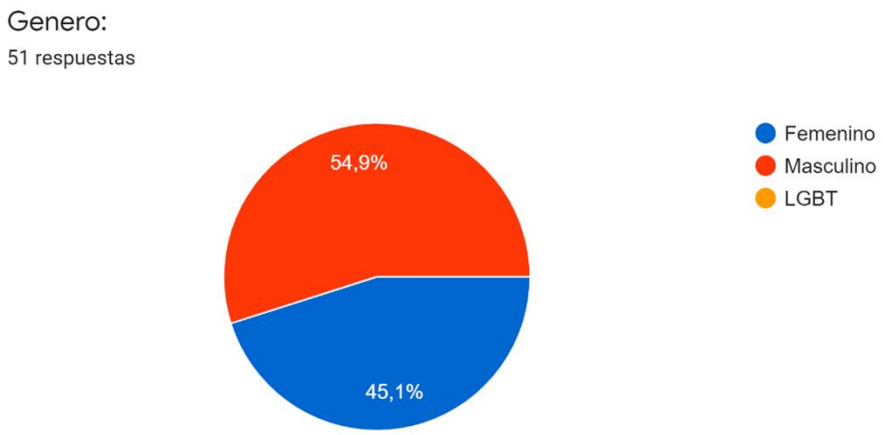
Opciones	Numeral	Porcentual
18-30	50	98%
31-40	1	2%
41-60	0	0%
60 o más	0	0%



2. Genero:

A. Masculino = 28
B. Femenino = 23
C. LGTB = 0

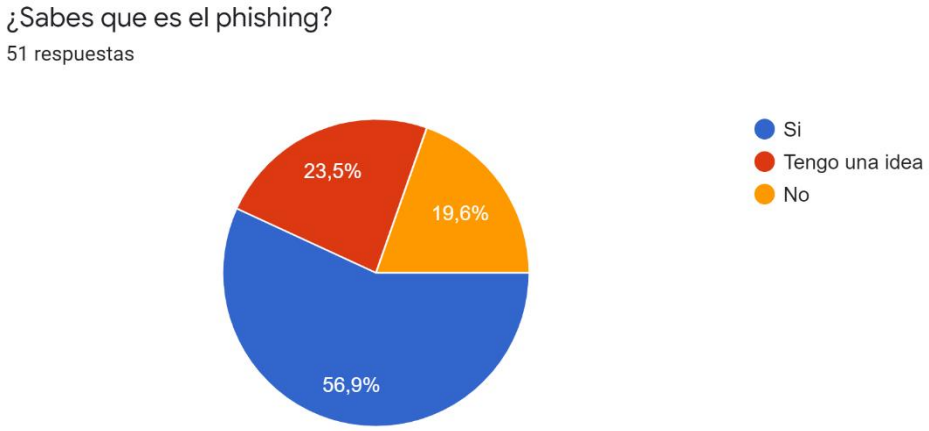
Opciones	Numeral	Porcentual
Masculino	28	54.90%
Femenino	23	45.10%
LGBT	0	0%



3. ¿Sabes que es el *phishing*?

A. Si = 29
B. Tengo una idea = 12
C. No = 10

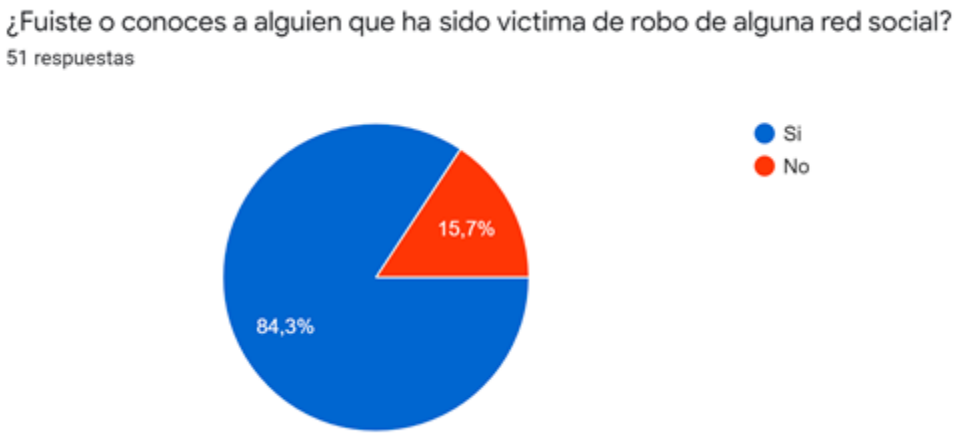
Opciones	Numeral	Porcentual
Si	29	56.90%
Tengo una idea	12	23.50%
No	10	19.60%



4. ¿Fuiste o conoces a alguien que ha sido víctima de robo de alguna red social?

A. Si = 43
B. No = 8

Opciones	Numeral	Porcentual
Si	43	84.30%
No	8	15.70%



5. ¿Te han intentado estafar o has sido estafado por alguien que dijo ser representante de algún banco?

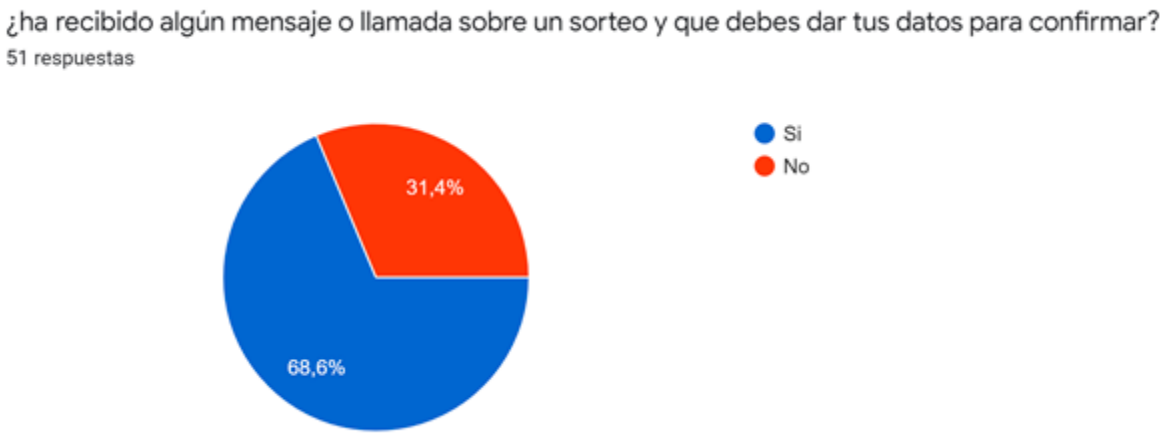
A. Si = 23
B. No = 28

Opciones	Numeral	Porcentual
Si	23	54.90%
No	28	45.10%

6. ¿Ha recibido algún mensaje o llamada sobre un sorteo y que debes dar tus datos para confirmar?

A. Si = 35
B. No = 16

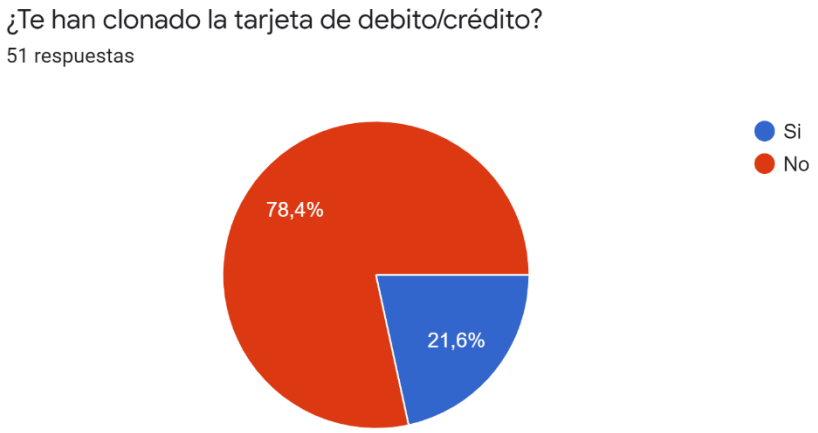
Opciones	Numeral	Porcentual
Si	35	68.60%
No	16	31.40%



7. ¿Te han clonado la tarjeta de débito/crédito?

A. Si = 11
B. No = 40

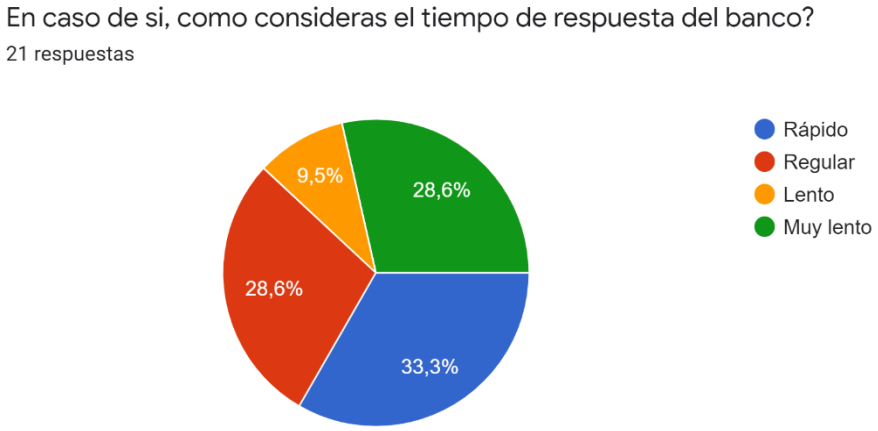
Opciones	Numeral	Porcentual
Si	11	21.60%
No	40	78.40%



8. ¿En caso de si, como consideras el tiempo de respuesta del banco?

A. Rápido = 7
B. Regular = 6
C. Lento = 2
D. Muy lento = 6

Opciones	Numeral	Porcentual
Rápido	7	33.30%
Regular	6	28.60%
Lento	2	9.50%
Muy lento	6	28.60%



9. ¿Te ha llegado algún e-mail falso con un link haciéndose pasar por alguna entidad financiera?

A. Si = 33
B. No = 18

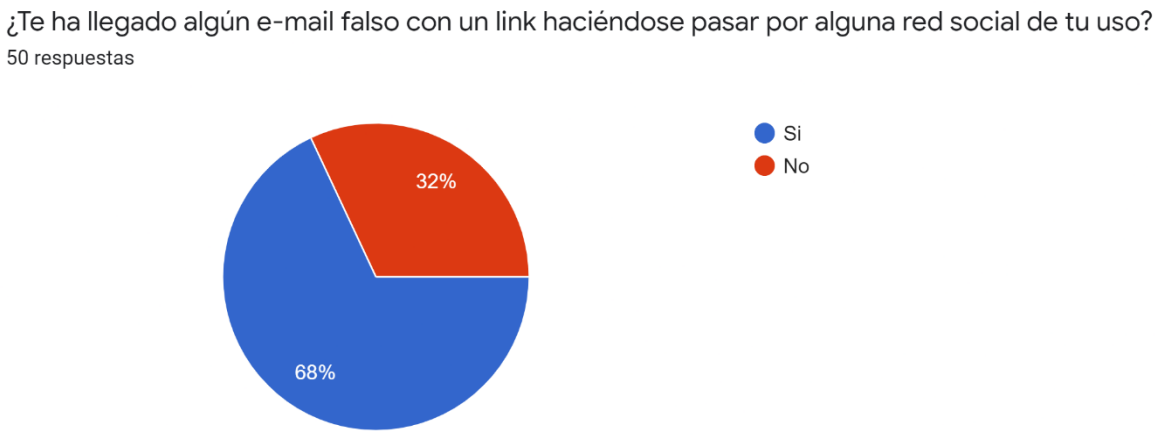
Opciones	Numeral	Porcentual
Si	33	64.70%

No	18	35.30%

10. ¿Te ha llegado algún e-mail falso con un link haciéndose pasar por alguna red social de tu uso?

A. Si = 34
B. No = 16

Opciones	Numeral	Porcentual
Si	34	68%
No	16	32%



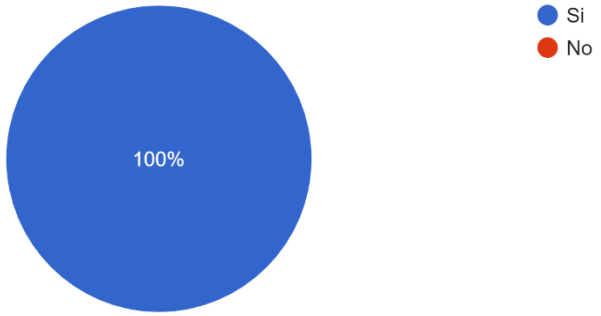
11. ¿Crees que debería el gobierno concientizar sobre el robo por *phishing*?

A. Si = 51
B. No = 0

Opciones	Numeral	Porcentual
Si	51	100%
No	0	0%

¿Crees que debería el gobierno concientizar sobre el robo por phishing?

51 respuestas



Anexo 2. Encuesta a expertos.

Interrogantes	Participantes	
	Participante 1	**Participante 2**
1. ¿Cuál es el estimado de denuncias recibidas de fraudes por usurpación de identidad que ha recibido esta institución desde enero del 2020 hasta julio 2021? (Si es posible el porcentaje de cada mes, desde enero 2020 hasta julio 2021)	Estas cifras son extremadamente confidenciales para el Banco, pero puedo decirte que recibimos aproximadamente entre 200 y 250 denuncias diarias de personas que son estafadas haciéndose pasar por empresas, que es un numero notablemente minúsculo comparado con las personas que nos denuncian consumos que no han realizado, los cuales oscilan muy por encima de las 8000 mensuales.	Estas cifras no pueden ser brindadas, ya que solo se utilizan con fines internos.
2. ¿Cuál es el estimado de denuncias por fraudes de usurpación que reciben mensualmente?	Como pude decirte anteriormente, entre denuncias de fraude y consumos no reconocidos, las cifras son muy superior a las 8mil denuncias mensuales.	Podría decirte que en este departamento recibimos por lo menos de 100 a 300 denuncias a nivel nacional diariamente, las cuales van desde denuncias de robo de identidad, robo de redes sociales y estafa.

3. ¿Qué porcentaje de estos casos pueden ser resueltos?	Se trata dentro del marco de lo posible, la solución de todos los casos, pero también dependerá de la participación de la víctima, y del nivel de cautela utilizada por el estafador. Un ejemplo sencillo es si la victima voluntariamente deposita el dinero en la cuenta de la persona que le está estafando, el proceso es totalmente diferente y el tiempo de respuesta del banco puede prolongarse.	No hay una cifra exacta, ya que cada caso puede ser más complejo que el anterior, pero se resuelven aproximadamente 50%, ya que hay casos que a veces son muy complejos.
4. ¿Cuál es la metodología más eficaz usada por los desaprensivos?	El envío de e-mails con links, los cuales te dirigen a una página falsa del banco, la cual es bastante semejante con la misma, y así hacerle creer que estos están en la página oficial, por lo que estos se sienten confiados en poner todos sus datos de acceso.	Generalmente utilizan el convencimiento, hacen creer que están llamando de algún Call Center, donde en ocasiones tienen conocidos los cuales le facilitan información personal de la víctima. Al momento de contactar a la víctima, el atacante pide la confirmación de los datos y pide las credenciales de la tarjeta de la víctima.