PROCESO DE ELABORACIÓN DE UNA INFOGRAFÍA TOMANDO COMO BASE DISTINTAS TÉCNICAS DE PHISHING

Anahí Rivas Valdez [1] Sánchez Arellano Guadalupe Graciela [2] Garzón Osuna Cynthia Paulette [3] Osuna Luna Daniel Ernesto[4] Medrano Mayorquín Itzamara[5]

[12345] *Facultad de Informática Mazatlán, Universidad Autónoma de Sinaloa (México)*

Resumen

En este artículo encontraras como el “Phishing” ataca a los usuarios y como prevenir un ataque mediante una infografía informativa, explicaremos sobre las diferentes maneras de combatir este problema y las medidas necesarias que un usuario debe tomar para no ser víctima de los delincuentes. Es un tema que involucra a la mayoría de la población debido a que cada vez realizamos más operaciones como transacciones, compras, ventas o registros a través de páginas web, que muchas ocasiones no conocemos la finalidad del porque nos piden este tipo de información.

1 INTRODUCCIÓN

En los años 90´s se dio a conocer la amenaza tecnológica llamada “Phishing”, en una empresa de Nueva York “AOL” empresa dedicada a los servicios de internet y medios. Los hackers se registraban con cuentas falsas utilizando algoritmos que generaban números de tarjetas de crédito que podían ser utilizadas por semanas e incluso por meses hasta que les requería una nueva. A medida que la empresa observo el problema en el año de 1995 tomo medidas de prevención, pero no fue suficiente ya que un hacker de AOL estaba enlazado con Warez que se dedicaba al software pirateado, este lo hacía por medio de un mensaje instantáneo que contenía textos de verificación de cuenta o confirmación de factura, una vez que el usuario aceptaba compartir su contraseña el atacante tenía acceso a la cuenta y ser utilizada para propósitos criminales como fraude, spam. Después de que esto no funcionara debido a que las empresas reforzaran su seguridad, capacitando a cada uno de sus empleados e informándoles sobre lo que estaba sucediendo, los phishers tomaron como su nuevo objetivo a clientes de bancos y servicios de pagos en línea debido a que era mucho más fácil engañarlos.

Hoy en día vivimos en un mundo moderno, la tecnología ha llamado tanto la atención tanto a niños como adolescentes debido a su facilidad de manejo y rapidez que ya es difícil no estar en contacto con cualquier medio de comunicación, actualmente queremos hacer todo por medio del internet, un ejemplo de ello sería cuando entramos a trabajar en una empresa, el administrador de dicha empresa ya no guarda nuestra información personal en carpetas y hojas de papel, sino que todo lo hace en forma virtual, esto quiere decir, en una base de datos, que estas están respaldadas por un sitio web para su seguridad pero esto también podría exponernos a que nuestros datos sean robados por personas que no estén autorizadas. Más de una persona que trabaje en una empresa o banco que haga transacciones mediante internet, habrán recibido correos electrónicos donde se les pide datos personales con solo decir que es para verificar datos en la empresa o para mayor seguridad, muchas personas han caído en esa trampa y revelan ciertos datos, datos que los ciberdelicuentes usan para hacer robo de su identidad y así poder cobrar cuentas en su nombre o pedir un crédito con el nombre y datos de la que fue su víctima, esto ha sido un gran problema que nos ha expuesto a muchas pérdidas de dinero o incluso llegar a participar en delitos graves teniendo como consecuencia muchos años de prisión y sin haber participado en ninguno de ellos.

Es necesario que estemos bien informados de algunas maneras de las que operan estos ciberdelicuentes para poder llegar a reducir la posibilidad de caer en su juego, pero

desafortunadamente no es posible estar protegido totalmente de este delito, porque cada vez los delincuentes ingenian nuevas estrategias para robar nuestros datos y usarlos con un mal fin, pero afortunadamente existen muchas técnicas para evitar caer en este problema.

En este artículo se pretende analizar los tipos de fraudes o crímenes informáticos que podrían existir dentro de la Universidad Autónoma de Sinaloa, ya que sería de gran utilidad para los alumnos que no cuenten con este tipo de información, beneficiando e informando al alumnado; así mismo para contar con una mejor capacidad de llevar un buen control en sus datos, documentos importantes, claves, de tal manera que se sientan tranquilos, hoy en día sabemos que muchas personas tienen la capacidad de filtrar información fuera o dentro de una empresa, escuela u otra institución y esto provoca una pérdida de datos importantes. Así se podrá tener una visión más amplia sobre la realidad de esta problemática, dando como resultado una infografía de un modelo de solución que sirva como punto de referencia para los universitarios y personal administrativo, con la finalidad de disminuir los riesgos y asegurar la integridad de la información de cada uno de ellos.

Pretendemos dar a conocer los fraudes y crímenes informáticos a toda la comunidad estudiantil por medio de este artículo y así la nueva generación que trascienda tenga una amplia capacidad y puedan desarrollar mejores propuestas de prevención de los tipos de robo, fraudes informáticos, etc. Para resolver el problema ya mencionado anteriormente crearemos una Infografía Informativa que es una combinación de imágenes sintéticas, explicativas y fáciles de entender y textos con el fin de comunicar información de manera visual para facilitar su transmisión, además de las ilustraciones, podemos ayudar al lector a través de gráficos que puedan entenderse e interpretarse instantáneamente. Con la creación de este artículo la comunidad estudiantil y administrativa de la Universidad Autónoma De Sinaloa estará informada de las amenazas de Phishing.

Con ello aterrizamos en el problema para resolverlo de la mejor manera describiendo y comparando las diferentes técnicas de Phishing, tomando como base los distintos estudios realizados con el fin de elaborar una infografía para mostrar al usuario información pertinente sobre las técnicas del robo de datos personales. De la misma manera conocer el significado, tanto en el campo del lenguaje como en el campo de la informática, conocer la forma en cómo se desarrolla y se pone en práctica, conocer la legislación vigente en la Universidad Autónoma de Sinaloa para la protección de la intimidad, la puntualidad de los fraudes e indicar a la comunidad estudiantil la amenaza informática que existe y prevenir y disminuir los ataques de Phishing.

2 METODOLOGÍA

Balestrini (2000) señala que el marco metodológico “es el conjunto de procedimientos a seguir con la finalidad de lograr los objetivos de la información de forma valida y con una alta precisión” (p.44). En otras palabras, es la estructura sistemática para la recolección, ordenamiento y análisis de la información, que permite la interpretación de los resultados en función del problema que se investiga.

Observando que el objetivo del estudio será analizar los tipos de soluciones que influyeron en la empresa en las cuales se utilizaran un diseño de investigación experimental, utilizando un enfoque cuantitativo.

El enfoque cuantitativo se utiliza la recolección y análisis de datos para contestar y realizar preguntas de investigación y confiar en “la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamientos en una población” (Hernández, Fernández & Baptista, 2003 p.5).

Del enfoque cuantitativo que se tomara la técnica de encuestas para medir la percepción de los ataques que fueron influyendo “Phishing” por parte de alumnos del campus Mazatlán, así como la opinión de ellos para la solución del problema.

Para resolver el problema se llevó una serie de pasos e investigación en la cual se dio a conocer que existe un índice alto de alumnos y personal administrativo del Campus de Informática Mazatlán que no sabe sobre este problema. La recolección de datos se dio con una muestra de 20 alumnos del lugar ya antes mencionado, así como también se les dará a conocer la información a la población del Campus de Informática Mazatlán. En el cual se estuvo preguntando si ellos conocían sobre este problema o si sabían que era. Con el fin de saber cuántas personas saben sobre que es el Phishing y cuáles son los métodos que se utilizarían.

Las técnicas de recolección de datos que se utilizara en la presente investigación será la encuesta, diseñado por preguntas cerradas bajo la escala de Likert. De este modo los instrumentos utilizados serian la investigación, aportes de marco teórico y las historias de como esto fue influyendo.

La escala de Likert es un instrumento de medición o recolección de datos que se dispone en la investigación social para medir actitudes, de acuerdo con Brunet (2004)”consiste en un conjunto de ítems bajo la forma de afirmaciones o juicios ante los cuales se solicitan la reacción (favorable o desfavorable, positiva o negativa) de los individuos” (p.34).

El paso primordial que se llevó a cabo en la investigación con la cual se generaron ideas, soluciones y problemas, que se solucionaron en el trayecto, un ejemplo seria la variación de información por la cual no se encontró una solución gratuita para acabar con el Phishing, en la cual se optó por una medida informativa y creativa para la sociedad estudiantil, ya que no está Informada sobre este acontecimiento.

Infografías	
Infografía informativa	Este tipo de grafico es conveniente para publicar noticias, explicar cualquier acontecimiento. Con la finalidad de ofrecer información actualizada y oportuna.
Infografía de producto	Sirve para describir los aspectos fundamentales de un producto, ya que ayuda a enfatizar las características más relevantes del producto.
Infografía secuencial	Esta muestra una secuencia de forma organizada. Utilizando una estructura en forma de lista con ayuda de iconos.
Infografía científica	Este facilita la enseñanza de temas científicos, pero no limita su uso de fines académicos.
Infografía biográfica	Este se emplea para hablar acerca de un fundador o de investigadores.
Infografía geográfica	Sirve para ubicar el lugar de un hecho por medio de mapas, su objetivo es indicar un trayecto geográfico de una persona.
Infografía de proceso	Propone un esquema visual y conceptual que permita entender paso a paso un tema o suceso.
Infografía cronológica	Muestra una sucesión de hechos o de datos respetando una línea temporal, es una forma de relatar una serie de manera ordenada.
Infografía estadística	Consiste en simplificar gráficamente la información numérica.
Infografía comparativa	Consisten en resaltar las diferencias entre elementos o variables, para orientar al público a tomar mejores decisiones.

Tomando en cuenta la información de las infografías antes mencionadas, se llegó a la conclusión de elegir la **Infografía Informativa** ya que esta nos ofrece el ser dinámica, entendible e informativa con la finalidad de ofrecer información oportuna y actualizada para que los estudiantes, personal administrativo/docentes puedan informarse de una mejor manera. Presentándose medidas preventivas para evitar caer en estos fraudes, añadiendo iconos con los medios principales de propagación, el tipo de información que roban y consejos breves de las acciones preventivas.

3 RESULTADOS

Con base a la información dada en la investigación acerca del Phishing, y teniendo conocimiento del grave problema que se enfrenta en la actualidad, se llegó a la solución de desarrollar una infografía informativa, que ayude al Campus de Informática Mazatlán, a prevenir este tipo de ataques. El significado y la armonía de los colores que se representan en la infografía son:

Color blanco: el blanco simboliza la pureza, la inocencia, en limpieza.
Color azul: el color del cielo, del mar, del agua, de la lejanía.
Color azul turquesa: simboliza la calma que se necesita para llegar a la inspiración. Color negro: asociado a la violencia, el misterio, la elegancia.

PHISHING

Una Amenaza Informática

Es un método que los ciber delincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

¿ Qué Tipo De Información Roban?

Datos Personales

- Números de documentos de identidad
- Direcciones de correo

Información Bancaria

- Números de cuentas
- Números de tarjetas de crédito

Credenciales De Acceso

- Redes sociales
- Cuentas de correo

Principales Medios De Propagación

- Correo Electrónico
- Redes Sociales
- SMS/MMS
- Llamadas
- Infección De Malware

ACCIONES PREVENTIVAS

Instituciones Confiables

Toma en cuenta que nunca solicitan datos mediante un email.

Enlace Sospechoso

No lo abras. Escribe en la barra de direcciones el nombre del sitio.

Verifica Autenticidad

Si sospechas del origen o contenido del correo.

Correo Electrónico Dudoso

Nunca des clic en los enlaces que contenga.

Verifica Tus Cuentas

Hazlo constantemente para poder evitar un pishing bancario.

Encuesta	
¿Qué es el Phishing?	**¿Cómo nos damos cuenta que somos víctimas?**
Tipo de información que roban	**Formas de prevenirlo**
En qué lugares se encuentran	**Técnicas de los ataques**

Las preguntas anteriormente mostradas son las que se realizaron a los alumnos con la finalidad de obtener un porcentaje de lo que ellos opinan sobre este problema que se está presentada mucho en la actualidad. Teniendo como resultado la información que se muestra en la siguiente tabla.

Resultado del Muestreo		
75% de los alumnos encuestados contesto que:	**13% de los alumnos encuestados contesto que:**	**12% de los alumnos encuestados contesto que:**
El orden de la infografía y los temas más importantes sobre este problema es el que se mostró anteriormente.	Todos los temas son importantes pero que debería de haber un software gratuito para el Campus de Informática Mazatlán.	No estaban enterados sobre esta gran problemática y que no llevaban a cabo compras por internet o simplemente no comparten sus datos personales-

4 CONCLUSIÓN

En medida del problema ya planteado concluimos en la infografía informativa ya que por medio de ella informaremos y actualizaremos la información día con día, ya que los usuarios no reconocían las medidas de precaución de los ataques del “Phishing”, la comunidad estudiantil se le informo y se le capacito como medio de prevención, logrando nuestro mayor objetivo de prevenir los ataques y la toma de medidas de precaución para no caer en las redes de los hackers.

Aunque muchas veces tenemos a disposición las herramientas que nos pueden ayudar a no ser víctima de los ataques la mejor manera de prevenir es la proporcionada por el usuario evitando abrir enlaces no confiables, llamados y no proporcionar información confidencial por medio antes mencionado. Además que día con día se descubren nuevas medidas de ataques y métodos de vulnerabilidad para los usuarios que más sofisticados.

5 REFERENCIAS

[1] http://paula-juliana-phising.blogspot.com/2016/07/la-historia-de-phishing.html?m=1

[2] https://blog.hubspot.es/marketing/tipos-de-infografias

[3] http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAQ6985.pdf

[4] https://es.venngage.com/

[5] https://es.scribd.com/document/97911790/El-Phishing-en-Apatzingan-c

[6] Lance James, Joe Stewart, Phishing Exposed, Secure Science Corporation, 2003, 381pp.

[7] Rachael Lininger, Russell Dean Vines, Phishing Cutting the Identify Theft Line, Wiley Publishing, Inc., India polis, 2005, 293pp.

[8] http://docs.media.bitpipe.com/io_11x/io_117740/item_972566/phishing-tacticses_W_newseal.pdf

[9] Oluwatobi Ayodeji Akanbi, Iraj Sadegn Amiri, Elahe Fazeldehkordi, A Machine Learning Approach to Phishing Detection and Defense, Syngress, Waltham, 2005, 81pp.

[10] AndaluciaCERT, Informe de divulgación Phishing, Junta de Andalucia, 2017, 22pp.

Mayra Sheila Mariana Leguizamón, Manuel Mollar Villanueva, El phishing, Universidad Jaume, 2015, 47pp.

[11] Ing. Aymara Noriley Belisario Méndez, Análisis de métodos de ataque de Phishing, Universidad de Buenos Aires, Facultades de Ciencias Economicas, 2014, 61pp.

[12] Maher Aburrous, Alamgir Hossain, Keshav Dahal, Phishing Website Detection Using Intelligent Data Mining Techniques, Lap Lambert Academic, 2012, 192pp.