MÉTODOS PARA EVITAR EL PHISHING, MEDIANTE EL USO DE LAS TECNOLOGÍAS

Rosa Leticia Ibarra Martínez[1], Mónica del Carmen Olivarría González[2], José Nicolás Zaragoza González[3], Sandra Olivia Qui Orozco[4], Oscar Sigifredo Otáñez Luna[5]

[1,2,3,4,5]Facultad de Informática Mazatlán, Universidad Autónoma de Sinaloa (México)

Resumen

En esta investigación ayudará a conocer sobre el método de estafa más popular en internet, el "Phishing", y se dará a conocer los métodos más eficaces para detectar cuando un simple correo electrónico es un posible hackeo y evitar este tipo de ataque considerado como un virus en Internet.

1 INTRODUCCIÓN.

Las Tecnologías de la Información y la Comunicación (TIC), como concepto general viene a referirse a la utilización de múltiples medios tecnológicos o informáticos para almacenar, procesar y difundir todo tipo de información, visual, digital o de otro tipo con diferentes finalidades, como forma de gestionar, organizar, ya sea en el mundo laboral [1].

El phishing, o la suplantación de identidad, uno de los delitos con más auge en la Red durante los últimos años, supone una importante amenaza para particulares y empresas. Las cifras hablan por sí solas: en 2012 se llevaron a cabo más de 37 000 ataques al mes. [2]

Hoy en día no hace falta ser ningún experto para cometer un fraude por Internet. Está al alcance de cualquier hacker que se lo proponga, gracias a las herramientas estándar de phishing que circulan por el floreciente ecosistema de la ciber delincuencia. Es más, los delincuentes informáticos están evolucionando hacia un nuevo modelo de negocio conocido como MaaS («malware como servicio»), en el que los autores de los kits de intrusión ofrecen servicios adicionales a sus clientes, además del kit propiamente dicho. [2]

Las consecuencias para las empresas pueden ser realmente graves. Según ha calculado RSA en su informe de fraudes publicado en febrero de 2013, las pérdidas a nivel mundial alcanzaron los 1500 millones de USD en 2012 y, si la duración media de los ataques hubiera sido similar a la de 2011, podrían haber llegado a los 2000 millones de dólares.Cualquiera que sea la amenaza ya sea que los empleados o clientes sean víctimas de un engaño, o que el sitio web de la empresa sufra una intrusión, la suplantación de identidad es un problema que hay que tener muy en cuenta. Las empresas deben estar al corriente de los modernos métodos empleados por los atacantes y adoptar las medidas preventivas necesarias para protegerse contra el fraude. [2]

El phishing el arte de atraer a internautas ingenuos para apoderarse de datos confidenciales, tales como nombres de usuario, contraseñas y números de tarjetas de crédito, mediante comunicados electrónicos en apariencia legítimos, supone una grave amenaza tanto para los particulares como para las empresas. Este tipo de fraude ha proliferado con rapidez desde su aparición hace diez años: se calcula que diariamente se cometen unos ocho millones de intentos de phishing en todo el mundo. En 2012, uno de cada 414 correos electrónicos enviados por la Red estaba relacionado con la práctica del phishing. [2]

2 PLANTEAMIENTO

El PHISHING comenzó en la década de los años 90, en esta década se presentaron los primeros casos del phishing, los que practicaron este delito en aquel tiempo lo hacían con el propósito de obtener algún beneficio por parte de las empresas pasándose por empleados a quienes le robaban la identidad para que la empresa les proporcione los servicios exclusivos de los empleados.

Con el tiempo este método ya no funcionaba por que las empresas comenzaron a reforzar la seguridad, capacitando al personal informándoles sobre lo ocurrido, después los phishers tomaron como objetivo a clientes de bancos y servicios en pago en línea.

El robo de identidad se da cuando una persona adquiere información de otra y la utiliza haciéndose pasar por ella, provocándole así un perjuicio. Este delito presenta una amplia connotación tecnológica, pero los esfuerzos por prevenirlos son de baja tecnología.

Actualmente jóvenes entre 15 y 30 años son los más vulnerables, pero nadie está exento. Las generaciones más jóvenes, publican sus datos personales y, la posibilidad de que estos sean utilizados en forma ilícita, son muchas, en la medida en que es mucha la información que se puede obtener de alguien a través de su perfil publicado.

[3]El fraude informático puede referirse, a medios electrónicos y redes de internet. Los sitios no seguros y falsos se convirtieron en un gran problema a nivel mundial, porque las compras en línea ofrecen muchas posibilidades sin salir del hogar.

[3]En la actualidad en el internet existen miles de sitios web que ofrecen una amplia variedad de productos y/o servicios, con un amplio descuento u ofrecen más artículos que otros sitios web.

[3]La mayoría de las veces sin darnos cuenta caemos en sitios que son un fraude o ignoramos la forma en que podemos ser víctimas de estos sitios, y las personas malintencionadas saben esto y toman ventaja de esto, creando sitios web falsos que parecen legítimos.

Los ciber delincuentes actúan muchas veces enviando e-mails (spam) donde se invita al usuario a recibir una determinada información. Al hacer click sobre los enlaces, es remitido a una página falsa donde le solicitan información personal que el delincuente recibe en su computadora.

Hay tantos avances en la tecnología informática y estas tienen gran influencia en la vida social de las personas, y han surgido acciones ilícitas que se conocen como delitos informáticos, los cuales con el desarrollo de la programación y el internet se han vuelto más frecuentes y sofisticados.

3 JUSTIFICACIÓN.

El Internet está a disposición de cualquier tipo de persona, como a su vez esta al alcance de los ciberdelincuentes, donde estas personas desarrollan diferentes métodos para robar y estafar, pero hay un método en especial que se llama phishing donde utilizan sitios web oficiales de empresas o instituciones, para engañar al usuario con enlaces falsos.

El resultado que se espera con esta investigación es que los usuarios aprendan a distinguir los sitios web falsos de los oficiales, porque de esa manera evitarán proporcionar su información personal.

El phishing está especializado en el método para robar tu información, a través del correo electrónico, donde su ataque comienza a través de un correo similar al de la empresa legítima o institución oficial.

4 METODOLOGÍA.

Objetivo General:

Evitar el redireccionamiento inconscientemente a un sitio web fraudulento cuando se trata de un usuario inexperto.

Objetivo Especifico:

1. Distinguir cuando es sitio web oficial de uno que no lo es.
2. Técnicas para evadir el phishing.

TIPO DE INVESTIGACIÓN.

El método de investigación aplicada es el que se utilizara en este protocolo, porque este método te ayuda a recopilar información más detallada sobre un tema en específico.

TÉCNICAS DE INVESTIGACIÓN.

La técnica que se está implementado en este protocolo, es la Técnica Documental, porque la información que se está recolectando es de libros, revistas, tesis y tesinas y sitios web.

OBJETOS DE RECOLECCIÓN DE DATOS.

El tipo de recolección de datos será mediante encuestas, porque de esa manera, se podrá analizar cuantas personas tienen el conocimiento sobre que es phishing y que métodos pondrán utilizar para evitarlo.

VARIABLES DE INVESTIGACIÓN.

- Variable Independiente: se le debe dar un uso adecuado a las Tecnologías.

- Variable Dependiente: phishing, mientras le des un buen uso a las tecnologías, disminuirán los ataques de phishing.

-

HIPÓTESIS.

La implementación de técnicas puede disminuir los ataques contra el Phishing.

5 CONCLUSION

Este protocolo tiene como objetivo, que las personas conozcan sobre el phishing, y como actúa.

La manera correcta de evitar estos ataques, es tener en cuenta de que manera actúan los proveedores de servicios financieros y otras entidades susceptibles de recibir este tipo de ataques. Estar informados de los nuevos ataques, para evitar las estafas que se realizan, porque es muy fácil caer en la trampa.

Y a medida que los usuarios estén bien informados y sepan cómo evitar estos ataques las victimas del phishing disminuirá.

REFERENCIAS

[1] Soler Pérez, V., El uso de las TIC (Tecnologías de la Información y la Comunicación) como herramienta didáctica en la escuela, en Contribuciones a las Ciencias Sociales, octubre 2008. www.eumed.net/rev/cccss/02/vsp.htm

[2] Symantec, Últimas tácticas de phishing y sus posibles consecuencias para las empresas, Libro Blanco Phishing, vol.1, no.10

[3] Juan G. Herramienta de evaluación de la seguridad de comercio electrónico [Tesis Licenciatura]. Ciudad de México: Instituto Politécnico Nacional; 2017.134 p.