Universidad Latinoamericana de Ciencia y Tecnología
Facultad de Ingeniería

Trabajo de Investigación: Las medidas de seguridad que toman los costarricenses sin conocimiento técnico y que utilizan cuentas de correo personales, frente a la ingeniería social

Por
Carlos Ortega

Resumen

El desarrollo de la tecnología no ha influido únicamente en facilitar las actividades diarias, sino, que ha propiciado actos delictivos que se valen de la falta de información e inocencia de los usuarios, la ingeniería social como punta de lanza usando la actividad conocida como *phishing*. Estas actividades generan todos los días pérdidas económicas considerables para diferentes sectores, empresas y particulares. Actualmente el *phishing* utiliza primordialmente el correo electrónico para enviar correos falsos por parte de los delincuentes informáticos. Estos correos piden claves, contraseñas o información de las cuentas bancarias objetando usualmente situaciones como problemas técnicos, procesos de actualización y revisión de datos tratando de aprovechar la ingenuidad de los clientes para obtener la información requerida. No se debe dejar de lado que en algunos casos las técnicas son más sofisticadas e implementa el uso de sitios web falsos para que el usuario piense que está en los sitios oficiales y así robar información. Ante esta problemática, Costa Rica por ejemplo no es ajena, ya que en los últimos años el OIJ ha reportado un incremento en el número de denuncias de fraudes electrónicos, donde participan costarricenses y que afecta tanto a los usuarios como a la banca nacional, donde el Poder Judicial ya ha resulto varios casos. Por ejemplo, solo el Banco Nacional tiene más de 250 mil cuantas de clientes en internet y más de la mitad de los ticos utiliza internet a diario, entonces surge una interrogante ¿Cómo protegen su información personal los costarricenses sin conocimientos técnicos, de la ingeniería social, en sus cuentas de correo electrónico? Según el estudio los participantes en la encuesta tienen pésimos hábitos usando su correo electrónico, los conceptos que conocen de seguridad son mínimos, en esta investigación se trata el tema y los resultados más afondo.

Abstract

The development of technology has not influenced solely to facilitate daily activities, but has led to criminal acts that rely on the lack of information and innocence of users, social engineering spearhead using the activity known as phishing. These everyday activities generate significant economic losses to different sectors, companies and individuals. Currently used primarily phishing e-mail to send fake emails by hackers. These emails ask for keys, passwords or bank account information such situations usually objecting to technical problems, processes for updating and review of data trying to exploit the naivete of customers to obtain the required information. You should not ignore the fact that in some cases are more sophisticated techniques and implements the use of fake websites to which the user thinks it is the official website and steal information. Faced with this problem, for example Costa Rica is not immune, since in recent years, IOJ has reported an increase in the number of reported phishing, where Costa Ricans involved and involving both users and the national bank, where the judiciary has resulted in several cases. For example, only the National Bank has more than 250 thousand internet few customers and more than half of Ticos use the Internet every day, then comes a question: how to protect your personal information Ricans non-technical, social engineering in their email accounts? According to the study participants in the survey are very bad habits by using your e-mail, known security concepts that are minimal, this research addresses the issue and the results more in depth.

Introducción

El mundo experimenta una era tecnológica muy agresiva, donde la manera de hacer las cosas ha cambiado casi por completo. Las sociedades han sido rodeadas por una gigantesca, poderosa y nueva transformación, donde lo virtual es la nueva realidad, personas de todas partes del planeta están conectadas al mundo de las redes sociales, correos electrónicos e internet en general, y el que no lo está, parece desactualizado, si de tecnología se trata. Esta tecnología evoluciona muy rápido, es una realidad, y se quiera o no, existe la necesitada de ajustarse a ella. En la actualidad millones y millones de personas de todo el mundo, utilizan cuenta de correo personal, inevitablemente un medio de intercambio de información y comunicación de tipo electrónica, y que es sencillamente una necesidad, más que un lujo, es una manera de estar presente en el mundo de Internet y las redes sociales. Por ello no es raro plantearse preguntas en esa dirección que nuestra mente formula, quizá nos preguntemos para que utilizan las personas esas cuentas de correo electrónico, que uso hacen de ellas, hasta donde puede ser peligroso usar el correo electrónico de servidores de correo gratuitos y cuando pueden convertirse en una verdadera amenaza. (Ávila Cruz VR 2005)

En tales circunstancias de un mundo que gira alrededor de la tecnología como un nuevo motor económico, social y cultural, y donde dicha tecnología es contagiada por los problemas que han enfrentado desde siempre las sociedades, debe mediar un cuidado especial, recordemos que quienes la utilizan siguen siendo hombres y mujeres, tan humanos como siempre. La tecnología vino a cambiar la forma de hacer las cosas, se habla de un cambio de paradigmas, pero que trajo a la vez nuevos problemas, consecuencia del nuevo modelo de vida. Junto a la tecnología, se vislumbra una manera diferente de delinquir, en este tiempo el ladrón no es solo aquel que espera por su víctima en la calle o aquel que ingresa a un banco armado, sino que

emerge una nueva forma de delincuencia, y que tiene un nombre bien identificado por los expertos. El robo de dinero, robo de números de tarjetas de crédito, peticiones de usuarios y claves personales, estafas, sustracción de información personal y todo engaño en un plano electrónico, surge debido a un fenómeno que utiliza como uno de sus medios los correos electrónicos, y que afecta a muchos usuarios en el mundo, hablamos de la poderosa y peligrosa Ingeniería Social. (Benigno Víctor 2006)

Según el especialista en ciencias informáticas, subgerente de Sistemas Informáticos de la Universidad Nacional de Rosario (UNR) Benigno Sánchez, la Ingeniería Social es la técnica por excelencia que tiene un Cracker (Delincuente informático) para realizar estafas y delitos electrónicos. Sin embargo, asegura que la tecnología en este caso no es el factor más vulnerable a los ataques de un Cracker, sino más bien, el factor humano, debilidades de los usuarios o el desconocimiento ante fenómenos de esta naturaleza. Por esta razón es importante y necesario conocer la preparación que tiene el ciudadano actual, en el uso de su correo electrónico y lo que hace para mantener segura su información. A nivel mundial la Ingeniería Social está creciendo, en Costa Rica por ejemplo, solo en el primer semestre del año 2009 se habían duplicado los casos de fraudes bancarios con respecto al 2008 (La Nación, 2009), las razones de este incremento en el numero de víctimas y de dónde viene el problema, son hasta ahora un tanto difíciles de enumerar. Estas peguntas son interesantes, de ahí que surge una gran interrogante ¿Cómo protegen su información personal los ciudadanos costarricenses sin conocimientos técnicos, de la ingeniería social, en sus cuentas de correo personales? Es sobre esta pregunta que se sustenta este escrito, con el fin de conocer un poco más el comportamiento de la población costarricense actual que utiliza correo electrónico, debido a la carencia de información concreta sobre este tema. Un objetivo claro es diagnosticar las prácticas de los costarricenses que no tienen conocimientos

técnicos, a la hora de utilizar sus cuentas de correo electrónico, con el propósito de obtener datos e información valiosa que beneficie a personas usuarias, entidades financieras, judiciales y otras de la sociedad costarricense.

Revisión bibliográfica

La proliferación y propagación de las actividades ilegales por medios electrónicos ha venido en aumento a nivel mundial en los últimos años, como resultado de una técnica como la ingeniería social, a través de la difusión de virus (McAfee). Esta técnica busca obtener datos confidenciales por medio de la manipulación de los usuarios propietarios de esta. Los delincuentes informáticos (Crackers) lo utilizan para obtener información y acceso a sistemas donde pueden obtener un beneficio personal, perjudicando a los usuarios u organizaciones de las cueles obtuvieron la información confidencial. El método preferido de los Crackers es la técnica donde a través de correos electrónicos engañan a los usuarios enviándoles links a páginas falsas (Phishing), ya sea de bancos, comercios e incluso de supuestas promociones, que en realidad contienen virus que son instalados en las computadoras de los usuarios. El objetivo primordial de este tipo de estrategia es capturar información de claves y cuentas de los usuarios titulares, para que el delincuente los utilice posteriormente como si este fuera el propietario de la cuenta. Una de los puntos fuertes de esta técnica es que los usuarios no saben que están siendo engañados, creen en todo momento que han utilizado los sitios oficiales de los bancos o comercios, enterándose tiempo después del problema, cuando ya han sido violentados. (Panda Security, 2010)

Para la Anti Phishing Working Group, organización encargada de luchar contra el Phishing, cada día los Crackers envían correos únicos a millones de cuentas de correo de usuarios en Internet, que apunta por lo general a un sitio web falso. También este organismo ha detectado millones de aplicaciones que intentan instalarse en las computadoras de los usuarios

para robarles información, o incluso para espiar las preferencias de los usuarios para luego vender esa información a diferentes agencias publicitarias. Tan solo en el segundo cuatrimestre del año 2010 la APWG recibió más de ochenta y cinco mil denuncias por medio de su cuenta oficial de correo electrónico de consumidores y socios que fueron víctimas de la ingeniería social. Además el número de sitios web dedicados al Phishing que lograron detectar es de más de noventa y siete mil, en el mismo periodo del año 2010, aunque con una tendencia a la baja con respecto al primer cuatrimestre del mismo año. Según el estudio de la APWG año 2010, el puerto 80 por medio del protocolo HTTP, que es el protocolo usado por los sitios web, es el preferido del los ataques Phishing, siendo esta una tendencia que se marca desde los inicios de los estudios desde el año 2003. Para el segundo cuatrimestre del 2010 más del 99 % de los ataques Phishing se produjeron por el puerto 80, a través de un sitio web, el otro uno por ciento se lo dividen el puerto 443 que es el puerto HTTPS, protocolo de transferencia segura de páginas web y el puerto 21 Protocolo de Transferencia de Archivos. Estos datos dejan claro que el uso de páginas webs seguras (HTTPS), son poco vulnerables a ataques, y por el contrario el protocolo HTTP es el medio por excelencia para producir la mayor cantidad de fraudes electrónicos. (APWG, 2010)

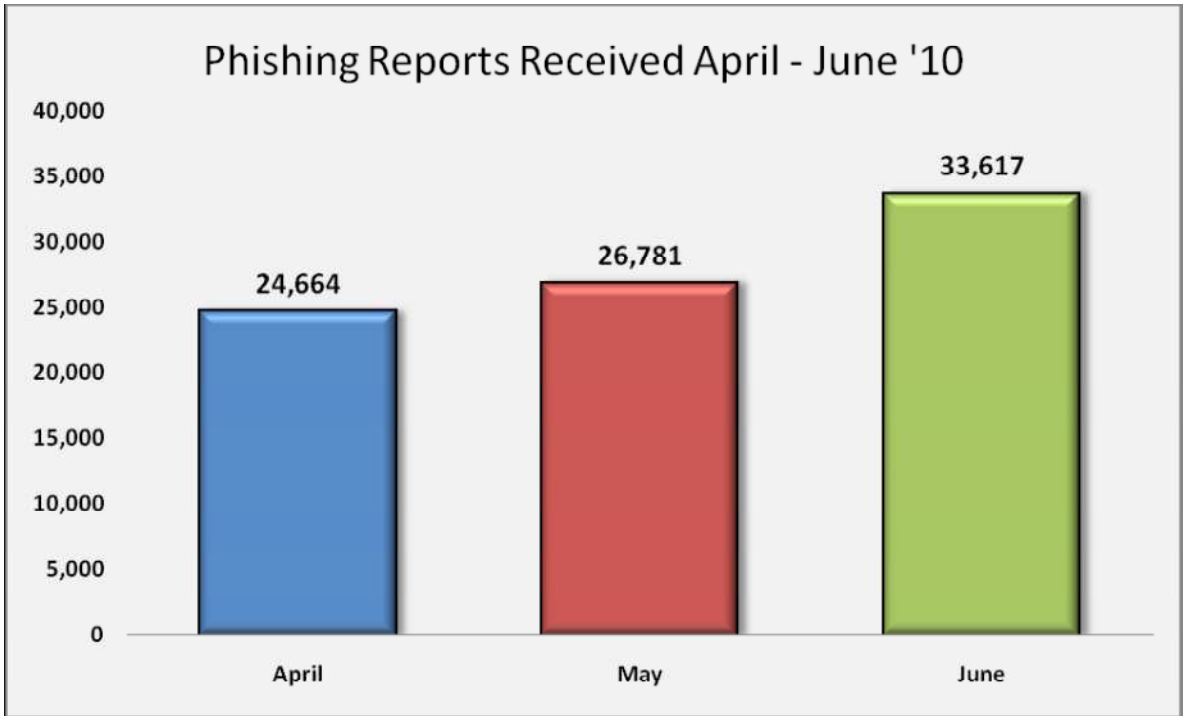

Grafico No.1. Cantidad de reportes de correos Phishing detectados en los meses de abril a junio del año 2010. (AFWG, 2010).

Cuadro numero 1
Cantidad de fraudes electrónicos perpetuados en los meses de abril a junio del año 2010, según el puerto utilizado

Abril		Mayo		Junio	
Port 80	99.92%	Port 80	99.88%	Port 80	99.46%
Port 443	0.06%	Port 443	0.09%	Port 443	0.41%
Port 21	0.02%	Port 21	0.03%	Port 21	0.13%

Nota: Most Used Ports Hosting Phishing Data Collection Servers – 2nd Quarter (APWG,2010)

Entonces, si se sabe que el protocolo HTTP es el más vulnerable a los ataques, ¿por qué sigue en aumento los casos de fraude electrónico?, en parte porque los timadores en Internet están constantemente innovando la manera de cómo engañar a la gente, haciendo cada día más sofisticados sus métodos, donde el correo electrónico Phishing es uno de esos métodos que siguen utilizando con frecuencia estos bandidos electrónicos. Para la compañía Microsoft los usuarios deben estar muy atentos a múltiples señales para evitar ser parte de las estadísticas de fraude o suplantación de identidad, que usualmente se utilizan en los mensajes de correo personal y que son estafas Phishing. Es importante recalcar que ninguna compañía, empresa o institución debe pedirle a sus clientes o usuario que proporcionen claves o nombres de usuario, ni ningún tipo de información personal por correo electrónico, porque normalmente son los timadores quienes realizan estas prácticas, haciendo parecer legitima la solicitud.

Los correos Phishing también pueden tener un tono amable, pero que denota algo de urgencia en la contestación, como puede ser que alarmen al usuario diciéndole que su cuenta va hacer cerrada en un determinado periodo, provocando que el usuario lo crea y conteste el correo. Otra de las maneras que suelen utilizar los timadores en los correos fraudulentos es la inclusión de un link dentro del correo electrónico que normalmente indica que es un link que dirige a una página segura, utilizan métodos para hacer creer que es una página verdadera pero es totalmente falsa. Según Microsoft los timadores también utilizan direcciones URL (nombres de los sitios webs), muy parecidos a los de nombre de compañías consolidadas y conocidas con el fin de hacer creer a las personas que es una página o dirección de dicha compañía. Una estadística destacada por la compañía Microsoft (2010, ¶ 4) dice que “De acuerdo con la encuesta State of the Net de Consumer Reports de 2005, las estafas de "phishing" en Estados Unidos tienen un costo medio de 395 dólares estadounidenses por incidente para los consumidores”

En Costa Rica la realidad no es muy lejana al panorama internacional sobre los fraudes electrónicos, tan solo en el año 2008 el Organismos de Investigación Judicial (OIJ) detuvo a 16 personas por fraudes mediante Internet. (La Nación, 2009). La manera de operar de los delincuentes electrónicos en Costa Rica es similar a la de los Crackers foráneos, por ejemplo, a nivel nacional se utiliza el Phishing de correos falsos a nombre de bancos estatales o privados del medio local y el Pharming, un método que envía tarjetas de felicitación por correo electrónico utilizado como medio para iniciar el robo de información. La Asociación de Comerciantes Libres, gremio de personas que han sido estafadas por medios electrónicos, estima que en los últimos años han sido afectadas por lo menos 900 personas, víctimas del atraco de sus cuentas bancarias. (OIJ, 2009). Las estadísticas del OIJ revelan que en Costa Rica se pasó de 120 casos en el año 2008 de estafas electrónicas a más de 243 en el año 2009, con más del 100% de incremento, siendo para las autoridades nacionales un repunte significativo de fraudes en contra de clientes principalmente de bancos públicos.(La Nación, 2009) .Según el OIJ los bandidos logran obtener por medio del Phishing o el Pharming los datos de los usuarios de las cuentas de bancos nacionales y proceden con la transferencia de fondos hacia otras cuentas bancarias, apareciendo como dueños de las cuentas destino, personas de escasos recursos principalmente del sur de San José, o jóvenes costarricenses que cuentan con beca del Fondo Nacional de Becas, y que prestan sus cuentas para dichos fines. Para las entidades bancarias costarricenses la situación es preocupante, porque Internet trajo muchas ventajas, pero también muchos de los riesgos que se están presentando en la banca electrónica, y es que el OIJ ha detectado que los timadores crean páginas web falsas a nombre de los bancos nacionales en servidores de China, Argentina y México, donde con toda seguridad hay ticos de por medio. (La Nación, 2009)

Para la banca nacional el tema de los delitos informáticos adquiere importancia, porque ellos son directamente afectados con cualquier problema que se presente a nivel de estafa electrónica, tal como lo ha venido resolviendo el Tribunal Contencioso Administrativo (Poder Judicial, 2011). El ente Judicial ha atribuido a los bancos la responsabilidad de los casos en los que se han realizado transacciones con claves de usuarios que dicen no haberlas realizado, y como resultado el banco ha tenido que indemnizar a los clientes. Los bancos han incorporado mecanismos de protección y seguridad, para minimizar posibles estafas, sin embargo la banca considera que la seguridad es responsabilidad no solo de quien brinda el servicio, sino también de usuarios y clientes particulares (La Nación, 2008). Pero según el Juez del Tribunal Contencioso Administrativo, Doctor Cristian Hess Hernández (comunicación personal, 18 de marzo de 2011) en Costa Rica existen una serie de regulaciones sobre delitos informáticos, por ejemplo la ley (7472) de protección al consumidor, que culpa a los bancos de las posibles vulnerabilidades, siempre y cuando la seguridad se rija por usuario y contraseña. Existe un proyecto de ley en la Asamblea Legislativa que está pendiente de aprobación, y que pretende robustecer la legislación actual, que de ser aprobada daría a la banca electrónica una serie de deberes y responsabilidades en este tipo de delitos. Como argumenta Hess Hernandez los bancos tienen la única salida para salvaguardarse de los fraudes electrónicos, en la implementación de certificados digitales (Ley 8454), porque haciendo uso de ellos la ley determina que quien tiene la culpa en un delito informático es el usuario y no el banco, como pasa actualmente. Entonces, sin duda llegará a ser importante para los usuarios el correcto manejo que hagan de sus cuentas de correos electrónicos, la administración de la información confidencial, y la seguridad que implementen para mantenerse protegidos de estafas electrónicas.

Métodos

En este estudio el instrumento utilizado para la investigación es La encuesta, la misma es del tipo cuantitativa, dicha encuesta consta de un total de 14 consultas, cuyas respuestas en su mayoría son de tipo cerradas. Se utilizó el formato de selección única, selección múltiple y preguntas estilo matricial. El cuestionario se elaboraron a partir de una serie de requerimientos considerados indispensables (Buenas prácticas) para medir los conocimientos necesarios que debe tener una persona para protegerse de ataques electrónicos. Una vez elaboradas las preguntas se procedió a realizar un pre testeo cognitivo con una muestra de 5 personas que hicieron sugerencias y preguntas de forma. El principal objetivo buscado con la aplicación de la encuesta, fue la de describir y medir actitudes y opiniones de usuarios sin conocimientos técnicos en el uso de las cuentas de correo electrónico personales, para obtener un análisis y conocer cómo protegen los ciudadanos costarricenses su información confidencial. Los datos obtenidos serán analizados para determinar los hábitos de dichas personas encuestadas para protegerse de la ingeniería social. Es decir, los resultados de este muestreo se pensaron para analizar el comportamiento de los usuarios a la hora de utilizar los correo electrónicos personales, y poder medir de alguna manera el grado de seguridad que implementan para protegerse de la ingeniería social, especialmente con los ataques Phishing y Pharming que se presenta en Costa Rica actualmente. La encuesta se aplicó de forma individual por medio de un documento impreso, que se entregó de manera personal, con una duración promedio para contestar la totalidad de las preguntas que rondó los 5 minutos.

La población encuestada en la muestra contemplaba tan solo dos restricciones, que fueran necesariamente personas sin conocimientos técnicos en informática y que dicha persona tuviera cuenta de correo electrónico, los individuos considerados para aplicar la encuesta fue una

población mayor de edad que va de desde los 18 años en adelante sin límite de suma, que podían o no, ser profesionales en otras áreas. Se encuestaron en la muestra un total de 50 personas, de los cuales el 52% fueron hombres y el restante 48% mujeres, que cumplieron estrictamente con lo planteado en el punto anterior. El tipo de muestreo utilizado en la encuesta es el tipo aleatorio, ya que se utilizó el azar como medio de elección de los participantes. No se puede decir con certeza que el muestreo sea del tipo probabilístico, porque no es posible garantizar a toda la población que cuenta con correo electrónico la misma probabilidad de ser elegidos en la muestra. Clasificando el tipo de muestreo puede decirse que es del tipo muestreo por conglomerados, por el hecho de que se utilizo diversas poblaciones que contaban con las características buscadas, siguiendo eso sí, el muestreo aleatorio dentro de cada grupo de individuos. Según La Nación en una encuesta de CID- Gallup para Radiográfica Costarricense, en Costa Rica aproximadamente 2,5 millones de personas se conectan a internet para revisar el correo, estudiar y chatear. (La Nacion, 2010) Tomando en cuenta este dato estadístico y la muestra de 50 personas que respondió la encuesta, con un nivel de confianza del 95%, se obtiene un margen de error del 14% aproximadamente en los resultados de la encuesta.

Resultados

De las 50 encuestas realizadas el 52% corresponde a hombres y el 48% a mujeres, con edades de entre los 18 años y los 50 años. A la pregunta de con qué frecuencia utilizan sus cuentas personales de correo electrónico los resultados dicen que el 92% de los usuarios lo revisa todos los días, un 8% al menos una vez por semana, lo que indica que por semana el 100% de los usuarios ingresan a su correo electrónico como mínimo una vez. Estos usuarios indicaron que los lugares desde donde suelen ingresar a revisar el correo electrónico son el hogar con un total de de 41 personas, el trabajo 39 de ellos, teléfono celular 15 personas y la universidad 12 personas, con

resultado muy bajo los accesos desde un café Internet es de apenas 9 de las 50 personas encuestadas. Adicionalmente según el uso que le dan a los correos el 78% de los encuestados respondieron que lo utiliza para fines educativos, y el 56% de ellos para redes sociales y un 38% para ocio y entretenimiento, también cabe destacar que de los encuestados el 40% de ellos aproximadamente, utiliza el correo para fines comerciales o compras online. Un 66% asegura usar la red social Facebook, el 56% utiliza el servicio de Messenger de Windows Live y alrededor del 30% tiene Skype o Twiter. Sin embargo, a la pregunta de si leen las condiciones de uso cuando deciden utilizar alguno de esos servicios mencionados anteriormente, el 74% aseguró que nunca las leen, contra un 26% que las leen completa o parcialmente.

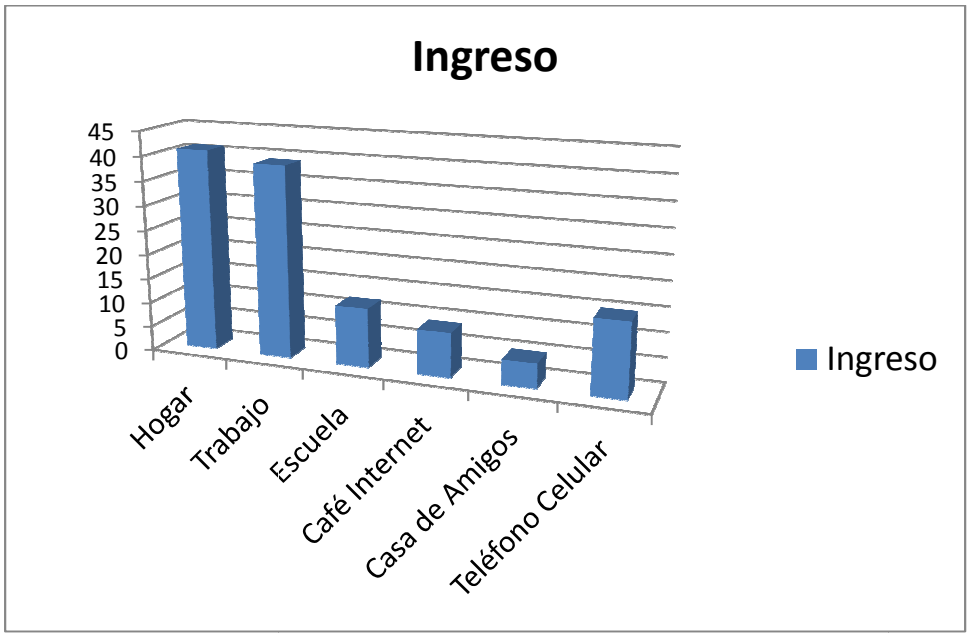

Grafico No.2. Muestra los lugares desde donde suelen ingresar los usuarios a la hora de revisar sus correos electrónicos, el hogar y el trabajo son los preferidos. Datos tomados del resultado de la encuesta.

Por otro lado, veamos lo que dijeron los usuarios con respecto a si creían que por medio del correo electrónico les pueden robar información personal y si lo consideran un medio con el que pueden ser engañados, con un contundente 98% los usuarios consideraron el correo electrónico como un medio en el que les pueden engañar y robar información. Paradójicamente el 28% de ellos comparte o ha compartido su clave personal de correo con otra persona, el 66% utiliza la misma clave del correo electrónico para otras aplicaciones y la mitad de ellos reenvía correos masivos sin saber si puede ser peligroso. Y si hablamos de conceptos de seguridad y uso adecuado del correo, más del 70% no conoce conceptos básicos como HTTPS (paginas seguras), certificado de seguridad (mecanismos para comprobar si un sitio web es seguro), además solo el 35% dijo saber lo que es una clave segura. Conceptos fundamentales como lo es ingeniería social, Phishing, Malware y SPAM más del 70% los desconoce o nunca ha escuchado de ellos y si hablamos de los cuidados en los equipos personales el 60% actualiza su antivirus, el 34% el navegador de internet y el 32% el sistema operativo, los demás nunca lo han hecho o no saben cómo hacerlo.

Discusión y conclusiones

A la luz de los resultados se puede ver que los usuarios aplican muy pocas técnicas y prácticas de seguridad para proteger su información personal, cuando usan sus correos electrónicos, aunque se reflejó que el 98% está consciente de que por medio del correo electrónico le pueden robar información confidencial, no se refleja que estos protejan de buena manera dicha información, no son consecuentes con lo que dicen saber y las prácticas que implementan. Por ejemplo, tal es el caso del porcentaje de personas que comparten su clave de

correo, resulta sumamente sorpresivo que casi 30% ha compartido la clave de su correo electrónico con otras personas, cuando es precisamente este uno de los objetivos de los delincuentes informáticos, obtener claves de cuentas de correo. Tal parece que los propios usuarios no saben cómo protegerse, no conocen la manera o no son realmente consientes de las consecuencias y se interesan poco. Como parte de los resultados se demuestra según la encuesta que los usuarios no tienen buenas prácticas con el uso del correo electrónico, porque muchos de ellos (hablamos de más del 60%) utiliza la misma clave de su correo electrónico personal en otras aplicaciones, ya sea en la red social Facebook, Messenger, Twitter u otros servicios, sin demostrar malicia al respecto. Esto sin duda se presta para que los correos de los usuarios sean vulnerables a ataques Hacker, pues es muy sencillo ingresar a las cuentas de sus correos una vez que se registraron en otras aplicaciones, teniendo acceso libre a la información confidencial, comprometiendo su seguridad y aumentando la posibilidad de sufrir un abuso de identidad.

Existen algunas reglas básicas que un usuario de Internet debe conocer para poder decir que navega seguro y que difícilmente puede ser víctima de un delito informático, o por lo menos que las probabilidades de serlo sean mínimas. Estas reglas por básicas que parecen pueden hacer diferencia, pero se demuestra que para muchos son desconocidas, no saben de su existencia, como muestra tenemos que una gran cantidad (86% de los encuestados) respondió que no conoce el significado de HTTPS, que sin duda es un mecanismo más seguro de navegar, muy utilizado por los bancos, comercios en líneas, y hasta servicios de correo como Hotmail, y que al no conocerse poco provecho se le puede sacar. El caso de las claves seguras, como buena práctica para la creación de claves, que son aquellas claves que contienen caracteres, mayúsculas, minúsculas y números; evidentemente es una práctica también desconocida por los usuarios y que no ponen en práctica en sus claves de correo personal, lo que sin duda minimiza la seguridad de

los correos y la información contenida en ellos. Muchos de los usuarios utilizan el correo para realizar compras online o para fines comerciales, lo que incrementa el riesgo de estafa o robo de número de tarjeta de crédito o de pin, pero ante esto los usuarios siguen demostrando ingenuidad y falta de cuidado porque un 70% no conoce lo que es un certificado de seguridad, mecanismo indicador de veracidad de las páginas web.

La ingeniería social de la que se habló al principio es, por lo menos para los encuestados, una práctica totalmente desconocida, la gran mayoría no conoce ni siquiera el concepto e incluso son incapaces de asociarlo a la tecnología. Es extraño que prácticamente todos los usuarios quienes a diario ingresan a revisar correo electrónico, visitan sitios de redes sociales, navegan en Internet, no conozcan si quiera lo que es la ingeniería social, siendo esta una de las herramientas de los Hackers. De 50 encuestados, solo 3 personas lograron identificar lo que es la ingeniería social y 13 dijeron que conocían el Phishing, al Malware solo 7 de ellos dijo saber que significa. Se evidencia aun más que los conocimientos en cuanto a los tipos de amenaza que se pueden encontrar las personas cuando navegan en la web y al utilizar el correo electrónico son desconocidas para la gran mayoría, dejando un amplio margen para que a futuro puedan ser víctimas de los delincuentes cibernéticos. Lo que se puede destacar es que para los usuarios el spam está bien identificado, conocen el concepto y toma algunas previsiones para no abrir este tipo de correos que según ellos son un tipo de virus que se instala en las computadoras y les puede causar daños, sin embargo, estos mismos usuarios son poco capaces de lograr identificar los correos Phishing o con virus pues poseen pocos o ningún conociendo al respecto.

Identificando entonces propiamente lo planteado al inicio de esta investigación, que hacen los usuarios sin conocimientos técnicos para protegerse de la ingeniería social en sus cuentas de correo, la respuesta a la luz de los resultados es muy lamentable, si lo vemos desde la óptica del

usuario que ni siquiera sabe lo que significa ingeniería social y que no puede reconocerla. Pero no todo es negativo, al menos los que suelen ingresar a Internet desde sus computadoras de casa realizan una práctica muy positiva, cuentan con antivirus instalado en sus computadoras y lo actualizan regularmente, también y aunque en menor medida actualizan el navegador y el sistema operativo, este ultimo solo 32% de ellos. Esto indica que muchos de ellos buscan protección para su información con la instalación de un antivirus y que intentan mantenerlo actualizado para evitar posibles ataques de virus nuevos. Esta es una de las buenas prácticas encontradas entre los usuarios consultados pero verdaderamente insuficiente para ser una barrera impenetrable e inviolable por los Hackers, ya que un buen antivirus trabajando en optimas condiciones no garantiza que no se den intromisiones de Malware o espías. Más de la mitad de los usuarios se consideraron que tienen un conocimiento intermedio o alto en el uso de correo electrónico y seguridad informática, hecho que se desmintió con los pocos conocimientos que demostraron de conceptos claves, y que se termina de evidenciar cuando vemos que muy pocas personas asisten a talleres o charlas sobre seguridad o lo que es peor no hacen nada para aprender del tema, y como único recurso consultan a algún informático conocido sobre hechos aislados.

Con este panorama se puede concluir que los usuarios que tienen cuentas de correo electrónico personal y que no poseen conocimientos técnicos, realizan poco para proteger su información confidencial. El nivel de conocimiento mostrado por ellos es muy pobre, los hábitos no son los adecuados para proteger dicho activo. Muchas veces y de manera en su mayoría inconsciente el usuario al participar en foros, blogs o gestores como Messenger, Facebook, entre otros, pueden proporcionar información personal, familiar o de terceros a gente que ni siquiera conocen, y que no saben el uso que le darán. Esto presupone sin duda un peligro, que según el

estudio los usuarios lo saben, pero no lo contrarrestan, pasan por ingenuos o confiados. Proporcionar datos a terceros (como claves) y darle el poder de medir nuestro comportamiento, nuestras preferencias para que sean vendidos a empresas no es algo ajeno a las redes sociales, que es muy usada entre los participantes en la muestra, estas malas prácticas de los usuarios y la confianza de cómo hacer un uso adecuado de las herramientas generan como consecuencia la posibilidad de que en algún momento sean parte de las estadísticas que el OIJ emite del aumento de estafas por internet. Por ejemplo, las compras online, trasferencias y otros usos de comercio electrónico, puede convertirse en un arma de doble filo para el usuario, primero porque facilita la vida, segundo porque puede ser engañado y estafado, esta vez, confianza es la problemática.

Otra de las conclusiones a las que se puede llagar con este trabajo es sin duda el poco conocimiento adquirido por los usuarios, es que un factor que puede desembocar en una estafa, engaño o robo de información personal, el no uso de las herramientas existentes para protegerse, hace al usuario más vulnerable a estos problemas. Aunque saben usar su correo electrónico y redes sociales poco saben de las consecuencias de un mal uso, y lo que es más grave nada hacen para adquirir conocimientos en ese sentido, pues la mayoría dijo que nunca ha realizado nada para aprender sobre seguridad. Entonces que se puede deducir de las anteriores líneas, que existe un camino que se debe recorrer para solventar muchas de las falencias que se presentaron en los usuarios encuestados. Los usuarios deben adquirir conocimientos básicos sobre seguridad, usar las buenas prácticas como normas de etiqueta en su diario vivir, esta es una de la formas que se puede paliar los riesgos de fraudes. Alertando a los usuarios de difundir sus datos personales y las repercusiones de hacerlo, concientizar a la población a adquirir conocimientos mínimos de seguridad y hacerles ver que el correo electrónico es tan personal como nuestra cuenta corriente, es la manera en que los usuarios corregirán las malas prácticas actuales. Las conclusiones y

recomendaciones denotan un cambio de paradigma, un cambio cultural, donde el usuario debe aprender a protegerse si quiere seguridad y debe ser pronto, esto para frenar la ola de fraudes de los delincuente informáticos que hacen todos los días de las suyas.

Bibliografía

Sánchez Curbelo, Benigno Víctor. (2006). Las nuevas tecnologías y los delitos informáticos. [En línea]. Consultado: [08, marzo, 2011]. Disponible en: http://web.ebscohost.com/ehost/detail?hid=9&sid=a95ca3a7-f671-402b-99d8-65250b2ca9b9%40sessionmgr10&vid=6&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#db=fua&AN=34162100

Otto Vargas. (08, febrero, 2009). Fuerte repunte en saqueo por Internet a cuentas bancarias. La Nación. [En línea], Español. Disponible: http://wvw.nacion.com/ln_ee/2009/agosto/02/pais2044433.html [2011, marzo 08].

Annabelle Ortega. (17, octubre, 2008). Responsabilidad ante fraudes electrónicos. La Nación. [En línea], Español. Disponible: http://wvw.nacion.com/ln_ee/2008/octubre/17/opinion1740635.html [2011, marzo 09].

Pablo Fonseca. (26, agosto, 2010). Más de la mitad de los ticos ya se conecta a Internet. La Nación. [En línea], Español. Disponible: http://www.nacion.com/2010-08-27/AldeaGlobal/NotasSecundarias/AldeaGlobal2499804.aspx [2011, marzo 18].

Microsoft Corporation (2010) ¿Qué es el "spear phishing"?. Recuperado el 7 de marzo de 2010 del sitio Web de Microsoft Corporation: http://www.microsoft.com/latam/athome/security/email/spear_phishing.mspx

Microsoft Corporation (2010) Contraseñas seguras: Cómo crearlas y utilizarlas. Recuperado el 10 de marzo de 2010 del sitio Web de Microsoft Corporation: http://www.microsoft.com/latam/protect/yourself/password/create.mspx

Microsoft Corporation (2010) Evite estafas de usurpación de la identidad. Recuperado el 10 de marzo de 2010 del sitio Web de Microsoft Corporation: http://www.microsoft.com/latam/athome/security/email/phishingdosdonts.mspx

Cormac Herley and Dinei Flor encio (2009) Phishing as Tragedy of the Commons. Recuperado el 15 de marzo de 2010 del sitio Web de Microsoft Research: http://research.microsoft.com/en-us/um/people/cormac/Papers/PhishingAsTragedy.pdf

Ronnie Manning, (2010) Phishing Activity Trends Report.Recuperado el 12 de marzo de 2010 del sitio Web de Anti-Phishing Working Group: http://www.antiphishing.org/reports/apwg_report_q2_2010.pdf

Panda Security, (2007) Spam, ingeniería social y malware. Recuperado el 18 de marzo de 2010 del sitio Web de Panda Security: http://www.pandasecurity.com/uruguay/homeusers/media/press-releases/viewnews?noticia=8426&entorno=&ver=20&pagina=5&producto

McAfee, (2011) McAfee predice el crecimiento de ataques en los que los cibercriminales explotan la naturaleza humana. Recuperado el 20 de marzo de 2010 del sitio Web Blog de WordPress.com: http://vulnerabilityteam.wordpress.com/contenidos/mcafee-predice-el-crecimiento-de-ataques-en-los-que-los-cibercriminales-explotan-la-naturaleza-humana/

Anexos

El instrumento

El presente cuestionario pretende diagnosticar el uso que le dan los usuarios sin conocimientos técnicos a sus cuentas de correo personales y como protegen su información. Le tomará alrededor de 5 minutos responderlo. Sírvase contestar con la mayor sinceridad posible, lo que se pretende es evaluar un comportamiento, ninguna respuesta es incorrecta.

1) ¿Cuál es su nivel como usuario de Internet y Correo Electrónico?

A) Básico B) Medio C) Avanzado

2) ¿Con qué frecuencia utiliza su correo electrónico?

A) Todos los días
B) Una vez al día
C) Algunos días de la semana
D) Una vez a la semana
E) Una vez al mes
F) Menos de una vez al mes

3) ¿Desde qué lugares suele ingresar a su correo electrónico? Puede marcar más de una opción

A) Hogar
B) Trabajo
C) Escuela/Universidad
D) Café Internet
E) Desde casa de amigos
F) Teléfono Celular

4) ¿Qué tipo de uso le da a su correo electrónico? Puede marcar más de una opción

A) Fines Educativos
B) Compras Online
C) Redes Sociales
D) Portales de Empleo
E) Ocio y Entretenimiento
F) Fines Comerciales
G) Otros _____

5) ¿Cuáles de los siguientes servicios utiliza? Puede marcar más de una opción

A) Windows Live Messenger
B) Yahoo Messenger
C) ICQ
D) Skype
E) Facebook
F) Twitter
G) Linked

6) ¿Siempre que decide utilizar algunos de los servicios de internet como los mencionados en la pregunta anterior lee las condiciones de uso completamente?

A) Sí lo leo
B) Nunca lo leo
C) No sabe / No contesta

7) De las siguientes condiciones acerca del correo electrónico, seleccione aquellas que ha realizado al menos una vez.

A) Compartir la clave con alguna persona
B) Permitir que otra persona vea cuando digita la clave
C) Reenviar correos masivos
D) Usar la misma clave del correo en otras aplicaciones

8) ¿Cree usted que por medio del correo electrónico le pueden robar información personal y puede ser engañado para proveer información confidencial?

A) Si B) No

9) ¿Conoce el significado de estos conceptos de seguridad?

	SI	**NO**
A) HTTPS	( )	( )
B) VeriSing	( )	( )
C) Clave Segura	( )	( )
D) Certificado de Seguridad	( )	( )

10) Antes de abrir un correo electrónico ¿Cuales características seria capaz de reconocer?

	Si	No
A) Si, es falso	( )	( )
B) Si, representa una amenaza	( )	( )
C) Si, contiene virus	( )	( )
D) Si, es Spam	( )	( )

11) ¿Conoce o ha escuchado sobre estos conceptos?

	Conozco	He escuchado pero no conozco	No conozco
E) Ingeniería Social	( )	( )	( )
F) Phishing	( )	( )	( )
G) Malware	( )	( )	( )
H) Spam	( )	( )	( )
I) Spyware	( )	( )	( )

12) ¿Cuáles de los siguientes elementos actualiza usted en su computadora?

	Si	No	Nunca	No se hacerlo
A) Antivirus	( )	( )	( )	( )
B) Navegador	( )	( )	( )	( )
C) Sistema Operativo	( )	( )	( )	( )

13) De las siguientes opciones: ¿Cuál describe mejor sus hábitos para adquirir conocimientos sobre seguridad y uso adecuado de Correo Electrónico?

A) Estudio Sobre el Tema
B) Consulta a Expertos
C) Asistencia a Talleres
D) Ninguna Hasta el Momento

Sexo:

1)Hombre 2) Mujer

Edad:

1) 18-25 años
2) 26-35 años
3) 36-50 años
4) Más de 50 años

Página para test de phishing para usuarios interesados en conocer su nivel de conocimiento en seguridad: **http://www.sonicwall.com/furl/phishing/**