UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN "SEGURIDAD INFORMÁTICA"

Tema:

"Guía de seguridades para prevenir el robo de la información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato"

Trabajo de Graduación. **Modalidad: SEMINARIO**, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Analuiza Lalaleo Luis Patricio

TUTOR: Ing. Clay Fernando Aldás Flores

Ambato - Ecuador

Diciembre-2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **"GUÍA DE SEGURIDADES PARA PREVENIR EL ROBO DE LA INFORMACIÓN POR MEDIO DEL PHISHING EN LA COOPERATIVA DE AHORRO Y CRÉDITO 10 DE AGOSTO DE LA CIUDAD DE AMBATO",** del Sr. Luis Patricio Analuiza Lalaleo, estudiante de la Carreara de Ingeniería en Sistemas Computacionales e Informáticos, de la facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad al Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Diciembre 2012

Atentamente,

…….

Ing. Clay Fernando Aldás Flores

AUTORÍA

El presente trabajo de investigación titulado: **"GUÍA DE SEGURIDADES PARA PREVENIR EL ROBO DE LA INFORMACIÓN POR MEDIO DEL PHISHING EN LA COOPERATIVA DE AHORRO Y CRÉDITO 10 DE AGOSTO DE LA CIUDAD DE AMBATO",** es absolutamente original, autentico y personal, en tal virtud el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Diciembre 2012

Atentamente,

…….

Analuiza Lalaleo Luis Patricio

C.I. 1803628203

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La comisión calificadora del presente trabajo conformada por los señores docentes Ing. Franklin Mayorga e Ing. Luis Solís, reviso y aprobó el informe final del trabajo de graduación titulado: **"GUÍA DE SEGURIDADES PARA PREVENIR EL ROBO DE LA INFORMACIÓN POR MEDIO DEL PHISHING EN LA COOPERATIVA DE AHORRO Y CRÉDITO 10 DE AGOSTO DE LA CIUDAD DE AMBATO",** presentado por el Sr. Luis Patricio Analuiza Lalaleo de acuerdo al Art. 18 del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

_____

Ing. Oswaldo E. Paredes O., M.Sc.

PRESIDENTEDEL

TRIBUNAL

_____ _____

Ing. Franklin O. Mayorga M. Ing. Luis A. Solís S.

Docente Calificador **Docente Calificador**

DEDICATORIA

Con la culminación de un peldaño más en mi vida quisiera dedicar este trabajo a Dios, a mis padres por su constante apoyo en los momentos más difíciles de mi carrera, a mi hija Zoe Maite para que sirva de ejemplo en su vida de lucha, perseverancia que recién está empezando a vivir y a toda mi familia que han sido un apoyo constante.

Luis Patricio Analuiza Lalaleo

AGRADECIMIENTO

Este es el momento propicio para expresar mi más profundo agradecimiento a la Facultad de Ingeniería en Sistemas por su gran labor enfocada a la formación de profesionales, al Ing. Clay Aldás, tutor del trabajo de graduación por guiar mis pasos en la ejecución, a la Cooperativa de Ahorro y Crédito 10 de Agosto por el apoyo, confianza y colaboración brindada.

Luis Patricio Analuiza Lalaleo

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El presente trabajo de investigación describe los capítulos en los cuales se desarrolla toda la información necesaria para obtener los resultados de la ejecución de la investigación realizada en la Cooperativa de Ahorro y Crédito 10 de Agosto.

Este trabajo es de gran importancia porque contribuirá con el desarrollo de la actividad económica financiera de la Institución, debido a que esta investigación pretende plantear una guía de seguridades para los usuarios de la Cooperativa 10 de Agosto, ya que existen muchas maneras de obtener información de usuarios de entidades financieras por medio del Internet, en nuestro caso utilizando un método llamado Phishing al cual vamos a realizar un estudio exhaustivo como es su funcionamiento y sus múltiples derivaciones.

INTRODUCCIÓN

Al proyecto "Guía de seguridades para prevenir el robo de la información por medio del phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato" que se presenta a continuación, se le ha dividido en capítulos que pretenden facilitar la comprensión del contenido de este trabajo.

En el primer capítulo se describe de manera general el tema de investigación de la Cooperativa de Ahorro y Crédito 10 de Agosto. Iniciando desde la problemática general que presenta sus respectivas variables generando un efecto negativo que afecta a la Institución y a sus socios.

En el segundo capítulo se detalla el marco teórico, el mismo que contiene toda la información general, comenzando con los antecedes, el problema de investigación que es la evaluación al proceso de navegación por medio del internet de los socios y los empleados de la Cooperativa 10 de Agosto.

El tercer capítulo hace referencia a la metodología aplicada en la investigación, los estudios necesarios a realizarse para sustentar la correcta ejecución, se establece el campo en donde se trabajará, la población y la muestra, y un análisis contencioso de las variables de investigación.

En el cuarto capítulo se ejecuta los parámetros necesarios con el objetivo de obtener resultados, los cuales nos provea la suficiente información para interpretar y verificar la hipótesis, lo cual rectifica que el estudio se aprueba la Hipótesis Alterna, por lo tanto se puede confirmar que la carencia de seguridades al momento de navegar en la web aumenta el robo de información de los socios de la Cooperativa de Ahorro y Crédito 10 de Agosto.

En el quinto capítulo se desarrolla las conclusiones y recomendaciones que se vierte del resultado de la ejecución de la investigación.

Finalmente en el **capítulo seis** se enmarca la propuesta del investigador, la cual está desarrollada en base a una investigación de los conceptos de todas los ataques que del método Phishing se derivan, además se toman referencias de los ataques realizados en otras entidades financieras, se toman las medidas y se establecen reglas para la navegación en la página oficial de la Cooperativa de Ahorro y Crédito 10 de Agosto.

CAPÍTULO I

1. EL PROBLEMA

1.1. Tema

Guía de seguridades para prevenir el robo de la información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato.

1.2. Planteamiento del problema

1.2.1. Contextualización

A nivel mundial se ha dado mucho lo que es el robo de la información mediante el Phishing, este tipo de delito informático ha venido creciendo constantemente debido al avance tecnológico mundial y a la accesibilidad que tiene la gente para estas tecnologías, así como avanzado la tecnología también han avanzado las amenazas y los peligros de la navegación por la web, es así que las personas que navegan en la Web son muchas pero con distintos objetivos, ya sean estos buenos o malos.

Algunos de los objetivos de usar la Web de buena manera son: la búsqueda de soluciones a problemas, enviar correos, realizar compras, realizar tareas, pagos de

servicios en línea, etc., pero también existen personas maliciosas que tratan de hacer el mal mediante la Web estos son: los hackers, lamers, Phishing, etc., los cuales tratan siempre de obtener la información de las personas para realizar ilícitos más conocidos como delitos informáticos estos pueden ser: suplantación de identidad, robo de los fondos bancarios, blanqueo de dinero, etc.

En los países subdesarrollados como el Ecuador, el uso de las tecnologías está creciendo significativamente, ya que un estudio realizado a nivel mundial revela que en el año 2008 el Ecuador ocupaba el puesto107 del desarrollo tecnológico mundial.

En el Ecuador el avance tecnológico ha servido para ser un país con muchas vulnerabilidades en cuestión de seguridades al momento de navegar en la Web y específicamente en las seguridades que debe tomar el usuario al momento de revisar sus cuentas bancarias o sus correos electrónicos, debido a que estos podrían acceder a páginas clonadas o ser víctimas de correos fraudulentos donde le piden información personal.

En Ambato existen pocos casos de fraudes bancarios por medio del Internet pero esto no quiere decir que no se deberían tomar medidas de precaución, en éste tipo de sociedad donde se pertenece a un país subdesarrollado, consumidores de tecnología son las sociedades que más propensas están a este tipo de delitos informáticos.

En la Cooperativa de Ahorro y Crédito 10 de Agosto se registra un bajo índice de pérdida de la información mediante la utilización del phishing como fraude informático debido a que en este año fue subida la página Web de la Cooperativa al Internet, además la Cooperativa ha visto la necesidad de prevenir y capacitar a los clientes sobre este tipo de fraudes o timos informáticos que se da por medio del Internet.

Si bien los índices de ataques por medio del Phishing son muy bajos dentro de la Cooperativa, así mismo las medidas de seguridades para prevenir este tipo de ataques también son muy bajos, además una de las causas por lo que se da este tipo de ataque es la mala navegación dentro de la página Web de la Cooperativa, un claro ejemplo son las señoritas cajeras de la Cooperativa que utilizan mucho las redes sociales como es el Facebook, twitter, etc. cuando se encuentran realizando sus actividades en la página Web de la Cooperativa, esto puede ser un problema muy grave si no se toma las medidas de seguridad al momento de navegar porque así los atacantes externos podrían estar robando la información de la Cooperativa o de sus clientes sin que la Cooperativa se diera cuenta.

1.2.2. Análisis crítico

Árbol de problemas

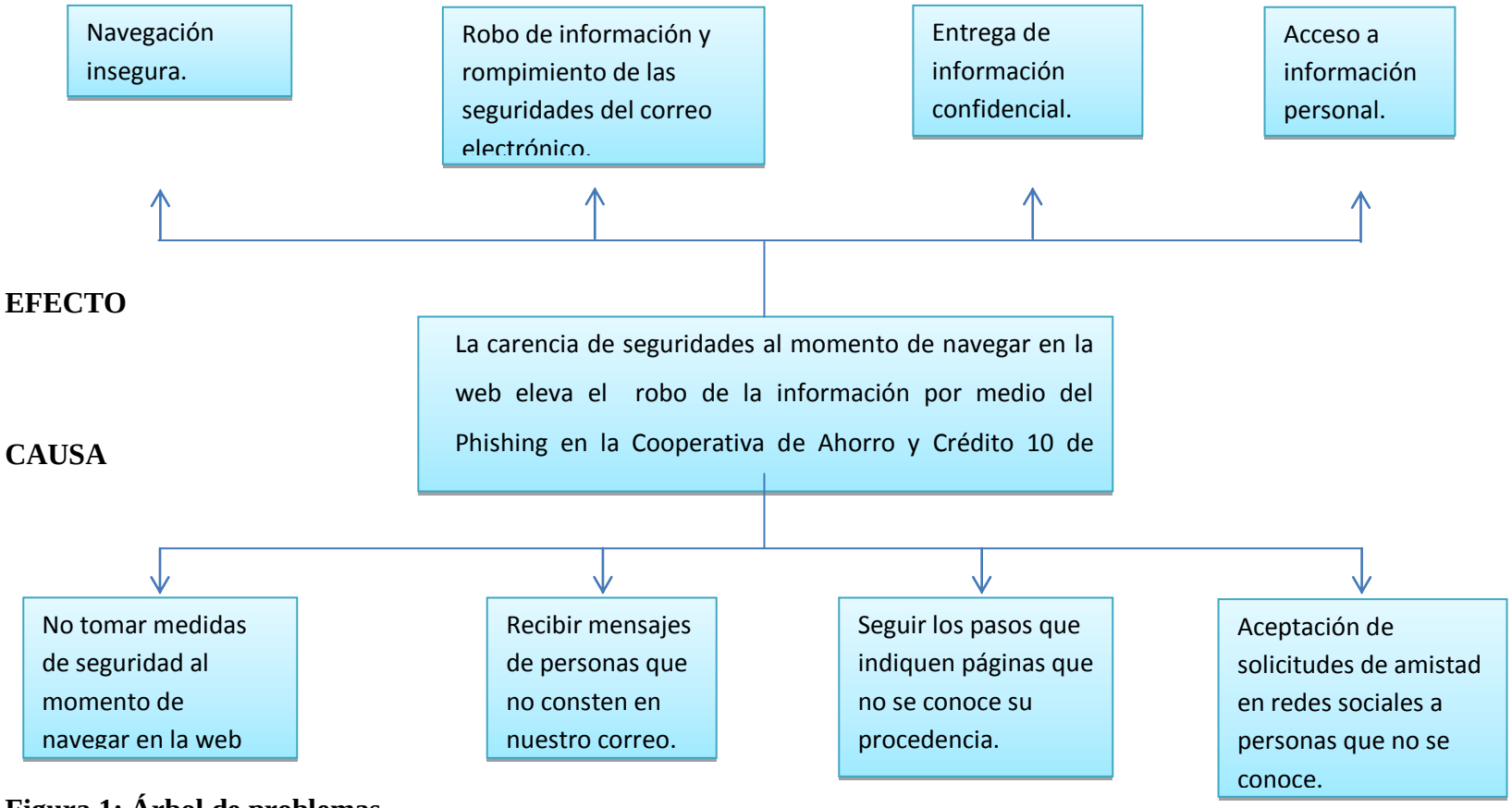


Figura 1: Árbol de problemas

La carencia de seguridades al momento de navegar en la web eleva el robo de la información por medio del phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto, una de las causas que debemos tomar muy en cuenta es que tanto los usuarios como los empleados de la cooperativa no toman las debidas medidas de seguridad al momento de navegar en la web esto provoca una navegación insegura, otra de las causas que se da es el recibir correos de personas que no consten en nuestros contactos provocando así el robo de la información como también el rompimiento de las seguridades de nuestro correo electrónico, por otro lado al momento de ingresar a páginas que no se conoce su procedencia se expone en gran parte la información personal que siempre debe ser confidencial, también el momento que se da la aceptación de solicitudes de amistad en redes sociales a personas que no se conoce se está dando acceso a nuestra información, todas estas causas influyen mucho al robo de nuestra información.

1.2.3. Prognosis

Si los empleados y clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato continúan sin el conocimiento acerca de las seguridades al momento de navegar en la web se tendrá muchos clientes estafados, suplantados de identidad por lo que generaría un conflicto entre los clientes y la Cooperativa de Ahorro y Crédito 10 de Agosto, además provocaría que los delitos informáticos sigan creciendo, por lo que la cooperativa perdería su prestigio, existiría perdidas económicas, afrontaría problemas judiciales y por consiguiente la empresa no tendría competitividad.

1.2.4. Formulación del problema

¿Cómo la carencia de seguridades al momento de navegar en la web eleva el robo de la información por medio del Pishing en la Cooperativa de Ahorro y Crédito 10 de Agosto?

1.2.5. Preguntas directrices

- ¿Cómo podría el usuario navegar de una manera segura en la web?
- ¿Cómo evitar ser víctima del robo de información mediante el Phishing?
- ¿Cómo se puede establecer las seguridades en la página web para proteger la información en la Cooperativa de Ahorro y Crédito 10 de Agosto?

1.2.6. Delimitación

Campo:	Seguridad Informática
Área:	Página Web y Correos electrónicos
Aspecto:	Guía de seguridades
Tiempo:	El estudio se lo realizara desde el año 2010 al 2011
Espacio:	Cooperativa de Ahorro y Crédito 10 de Agosto

Tabla 1: Delimitación

1.3. Justificación

La guía de seguridades para prevenir el robo de la información en la Cooperativa de Ahorro y Crédito 10 de Agosto es de mucho interés para la colectividad del centro del país, debido a que este tipo de fraude está tomando auge a nivel nacional y mundial por lo que nuestra sociedad deberá estar prevenida de este tipo de ataques por lo que se creara una aplicación llamada Phishing para enviar un ataque a todas las personas que cuenten con una cuenta de correo electrónico y una cuenta en la cooperativa para obtener un análisis estadístico de todas las personas vulnerables a este tipo de ataques, luego se realizara una aplicación donde indique todos las posibles preguntas que realiza un Phisher al momento de enviar el ataque y así evitar que el usuario sea una víctima más de este tipo de delito informático.

El tema es novedoso debido a su reciente aparición en nuestro medio y creo que tendrá un impacto muy favorable en nuestra sociedad debido a que nosotros somos una sociedad consumidora de tecnología pero no tomamos las debidas seguridades al momento de utilizar estas tecnologías de una buena manera, así pues los beneficiarios de esta investigación será la colectividad del centro del país porque finalizada esta investigación el usuario de la tecnología sabrá cómo protegerse de este tipo de ataque informático.

La investigación a realizar es factible porque se posee información y medios para realizar el trabajo además será muy útil para la sociedad del centro del país y en especial para los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto.

1.4. Objetivos

General

Elaborar una guía de seguridades a través de un estudio del Phishing para prevenir los robos de información.

Específicos

- Determinar las formas que se utilizan para navegar en la página oficial de la Cooperativa de Ahorro y Crédito 10 de Agosto.
- Establecer herramientas informáticas de seguridad para detectar páginas fraudulentas o correos maliciosos.
- Diseñar una guía de seguridades para prevenir el robo de información en la Cooperativa de Ahorro y Crédito 10 de Agosto.

CAPÍTULO II

2. MARCO TEORICO

2.1. Antecedentes Investigativos

Después de realizar la Investigación en los archivos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato no se da conocer trabajos de investigación similares al tema propuesto por mi persona.

2.2. Fundamentación legal

CONSTITUCION DEL ESTADO ECUATORIANO

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

Sección octava
Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.
3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 387.- Será responsabilidad del Estado:

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, alsumakkawsay.
3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.
4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y

desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

Sección novena
Gestión del riesgo

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.
4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.
5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.

6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidades y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.

2.3. Categorías fundamentales

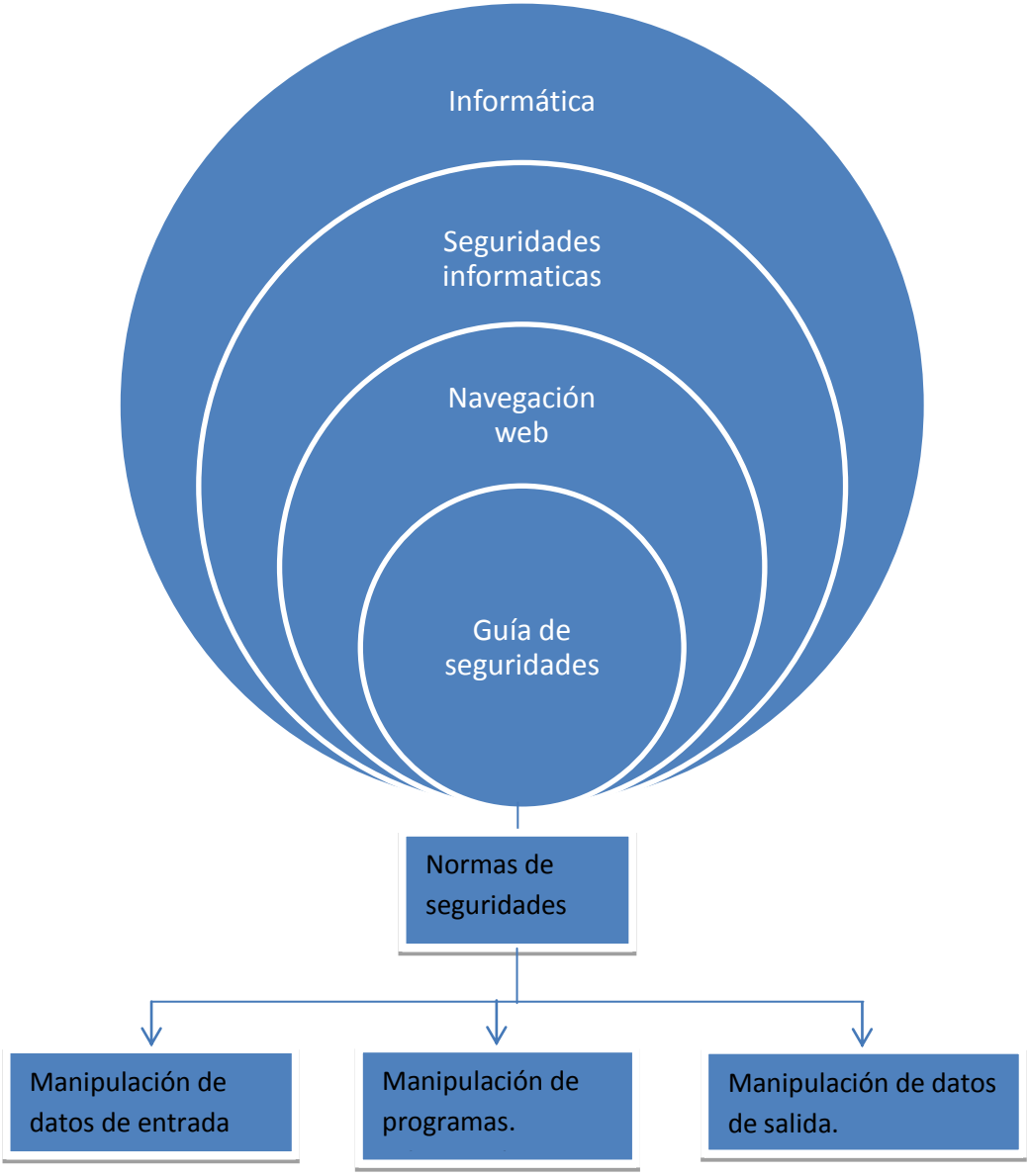


Figura 2: Variable independiente

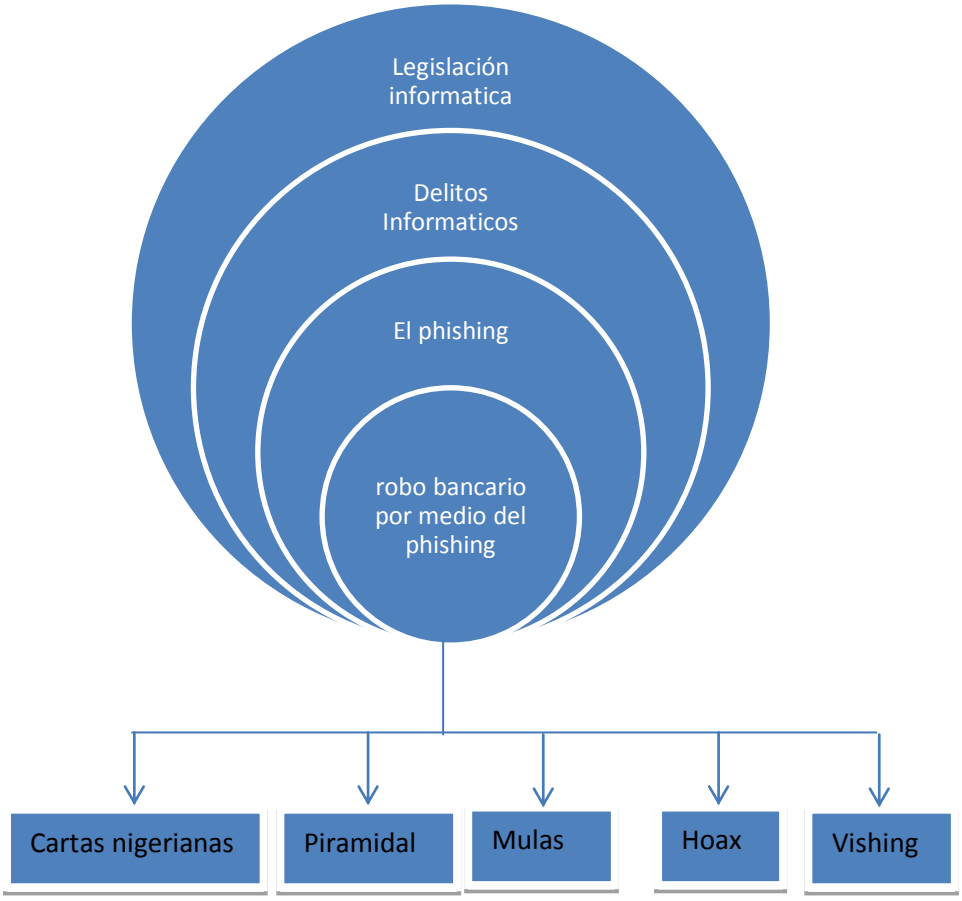


Figura 3: Variable dependiente

Informática

1. Según la monografía de ellos (Internet, 2009, 28 oct 2011, a las 8:52). "El término informática proviene del francés "informatique", que a su vez se deriva de la contracción de dos palabras: "Información" y "automática", y se define como el conjunto de disciplinas y técnicas que se encargan del tratamiento automático de la información."
2. Por otro lado la página de GarballeCollector (Internet, 05/04/2004, 28 /10/ 2011, a las 10:13). "Como definición de informática se suele aceptar "ciencia que estudia el tratamiento automático de la información". El término procede del francés "informatique" formado a su vez por la conjunción de las palabras

"information" y "automatique". No obstante en sudamérica, se suele utilizar más la palabra "computación", más cercano a la expresión anglosajona de "ComputerSciences" (CS) o ciencias de la computación."

3. Por su parte Federico Martín Maglio (Internet, 20/03/1999,28 /10/ 2011, a las 10:21). "La informática es un recurso didáctico y abarca al conjunto de medios y procedimientos para reunir, almacenar, transmitir, procesar y recuperar datos de todo tipo. Abarca a las computadoras, teléfono, televisión, radio, etc... Estos elementos potencian las actividades cognitivas de las personas a través de un enriquecimiento del campo perceptual y las operaciones de procesamiento de la información."

La informática es un recurso que deriva de las palabras información y automática y se encargan del tratamiento de la información y su procesamiento.

Seguridades informáticas

1. Una versión de la página Mastermagazine. (Internet, 2011, 28 /10/ 2011, a las 10:39). "Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática."
2. Según el pdf de anónimo (Internet, 2010, 28 /10/ 2011, a las 10:35). "La seguridad en la web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios del Web y las organizaciones que los rodean. La Seguridad es una protección contra el comportamiento inesperado."
3. Por su parte la opinión de Gestión de riesgo en la Seguridad Informática (Internet, 2010, 28 /10/ 2011, a las 10:44). "La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad."

La seguridad informática es un conjunto de procedimientos que permiten proteger la información confidencial así como su integridad.

La web

1. Según Definición de (Internet, 2011,04/11/2011,7:25). "Un *weblog* es una página *web* de fácil actualización. Sí, tienen esa característica que les permite a los autores de *weblogs* publicar contenido (textos, imágenes y otros archivos) con apretar un solo botón. Cualquiera puede editar un *weblog* gracias a la cantidad de herramientas que hay en la web para hacerlo. Esta herramienta se conoce, por lo general, con el nombre de gestor de contenidos o *Content Management System* (CMS). Con esta herramienta puedes actualizar tu página desde cualquier ordenador con acceso a Internet."
2. De acuerdo con la Definición de (Internet, 2011,04/11/2011,7:25). "Navegación, del latín *navigatĭo*, es la acción, la ciencia y el arte de navegar. Este verbo refiere a viajar en una embarcación o a hacer un viaje por aire, aunque también puede hacer referencia al desplazamiento a través de una red informática."
3. Por su parte masadelante.com (Internet, 2011,04/11/2011,7:30). "En inglés website o web site**,** un sitio web es un sitio (localización) en la World Wide Web que contiene documentos (páginas web) organizados jerárquicamente. Cada documento (página web) contiene texto y o gráficos que aparecen como información digital en la pantalla de un ordenador. Un sitio puede contener una combinación de gráficos, texto, audio, vídeo, y otros materiales dinámicos o estáticos."

La navegación web se refiere a navegar entre páginas en internet las cuales permiten recibir y enviar información así como realizar transacciones bancarias o recepción de correos.

Guía de seguridades

1. La página de Slideshare (Internet, 2010,04/11/2011,7:40). "La guía de actividades es importante porque nos da las pautas y directrices para el desarrollo de las acciones y poder ejecutar el trabajo encomendado con éxito."
2. Según Anónimo (Internet, 2001,04/11/2011,11:24). "Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible."
3. Según la página de CiberHabitat(Internet,04/11/2011,11:24). "Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática."

Es un conjunto de normas, reglas y procedimientos para la navegación en el internet, debido a que permite evitar ser víctimas de ataques informáticos y Mantener las operaciones eficientes.

Norma

1. Según la Definiciónde (Internet, 2011,04/11/2011,11:37). "**Norma** es un término que proviene del latín y significa **"escuadra"**. Una norma es una **regla** que debe ser respetada y que permite ajustar ciertas **conductas** o actividades. En el ámbito del **derecho**, una norma es un precepto jurídico."
2. Por otro lado Wikipedia (Internet, 8/10/2011,04/11/2011,11:40). "En Derecho, una norma jurídica es una regla u ordenación del comportamiento dictada por una autoridad competente, cuyo incumplimiento trae aparejado una sanción."
3. Según Buenas tareas (Internet, 3/11/2011,04/11/2011,11:46). "Norma que establece las disposiciones en materia de seguridad informática."

Norma es un conjunto de procedimientos ordenados que permiten tener una mejor estructura para realizar una cierta actividad.

Fraudes informáticos

Según el criterio de CARRION, Hugo (Internet; 01/07/2001; 25/10/2011; 14:10 PM), dice que existen varias maneras de cometer fraudes informativos entre ellos:

1. **"Manipulación de los datos de entrada:** Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir."
2. **"Manipulación de programas:** Consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación."
3. **"Manipulación de los datos de salida:** Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos."

Debido a los conocimientos de los distintos expertos se puede concluir que existen diversas formas de cometer fraudes informáticos: manipulación de datos de entrada como por ejemplo al ingresar datos falsos en un sistema, manipulación de sistemas, es decir cambiando las instrucciones propias de los programas para que realice acciones que beneficien al delincuente como por ejemplo desvió de transacciones y manipulación de datos de salida como por ejemplo falsear la información que observamos en los cajeros automáticos.

Legislación Informática

1. Una opinión de Troyaurora (Internet, 2011, 04/11/2011,12:02). "Se define como un conjunto de ordenamientos jurídicos creados para regular el tratamiento de la información. Las legislaciones de varios países han promulgado normas jurídicas que se han puesto en vigor dirigidas a proteger la utilización abusiva de la información."
2. Según Informática jurídica (Internet, 16/10/2010, 04/11/2011,12:08). "Constituye una ciencia y rama autónoma del derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) Regulación del medio informático en su expansión y desarrollo y b) Aplicación idónea de los instrumentos informáticos.
3. Por otro lado Wikipedia (Internet, 15/10/2011, 04/11/2011,12:28). "Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática."

Legislación informática son normas establecidas en la ley para castigar los delitos informáticos.

Delitos Informáticos

Según Legislación informática (Internet, 14/06/2010, 04/11/2011,12:22). "

1. El autor mexicano Julio Téllez Valdez señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".
2. Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo."

3. El autor Davara Rodríguez lo define como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware osoftware."

Los delitos informáticos son fraudes o timaciones que se lo hace mediante la utilización de páginas de internet.

El Phishing

1. Según el Diccionario informático (Internet, 04/11/2011, 04/11/2011,12:32). "El phishing es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. El objetivo más común, suele ser la obtención de dinero del usuario que cae en la trampa."
2. Por otra parte Seguridad.net (Internet, 28/10/2011, 04/11/2011,12:34). "PHISING consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas."
3. Un Anónimo (Internet, 28/10/2011, 04/11/2011,12:34). "Según Wikipedia "es un término informático que denomina el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria)"

El Phishing es un tipo de delito informático el cual utiliza mucho lo que es el correo electrónico y el re direccionamiento de páginas de entidades bancarias.

Robo bancario

Según el reloj.com (Internet, 28/10/2011, 04/11/2011,12:54). "Un banco sueco tiene el triste récord de contar con el mayor fraude informático de la historia. La entidad Nordea sufrió el ingreso de unos ciberladrones que se llevaron 880 mil euros."

Consiste en el envío de correos electrónicos que aparentando provenir de entidades bancarias **intentan obtener datos confidenciales del usuario.** Para esto, suelen incluir un enlace que lleva a páginas web falsificadas.

Cartas Nigerianas

Carlos cabezas (Internet, 03/09/2007, 04/11/2011,13:50). "El de la "lotería nigeriana" tal vez sea uno de los timos más comunes que pueden llegarse a ver en los correos electrónicos de usuarios de todo el mundo. Súbitamente y de la nada, un mensaje, con un supuesto membrete oficial de la Lotería de Nigeria, llega explicando que la futura víctima se ha hecho beneficiaria de un premio millonario."

Estafa Piramidal

La página de PaperBlog (Internet, 04/11/2011, 04/11/2011,14:07). "Esta estafa está muy de moda en estos momentos, teniendo en cuenta el momento de crisis en el que se encuentra el país. El usuario recibe una oferta de empleo en su correo electrónico, basada en la promoción de productos y en la captación de nuevos empleados. Los nuevos empleados tienen que abonar una tasa de iniciación para poder trabajar, que evidentemente nunca recuperaran, y a la hora de la verdad descubriran que los beneficios obtenidos se generan por la captación de nuevos miembros, y no por la venta o promoción de productos.

Mulas

Por su parte PaperBlog (Internet, 04/11/2011, 04/11/2011,14:07). "Este timo es grave, ya que puede suponer la cárcel para el que caiga en él, al tratarse de un delito de blanqueo de dinero. El usuario recibe un correo electrónico con la posibilidad de quedarse con un porcentaje de una transacción electrónica únicamente por realizar una transferencia del importe recibido menos su comisión a otra cuenta que se le indica. Hay que tener mucho cuidado con estas proposiciones y hay que preguntarse por qué no puede hacer esa transferencia directamente la persona que lo solicita. Si no puede hacerla él mismo por algo será."

Hoax

La página PaperBlog (Internet, 04/11/2011, 04/11/2011,14:07). "Se trata de timos o bulos que en muchos casos se utilizan para sensibilizar al usuario para que realice aportaciones económicas, aunque no siempre existe este componente económico. Para ello, se utilizan numerosos recursos, como aprovechar las noticias de la actualidad (últimamente, por ejemplo, se ha utilizado el recurso de la ayuda a **Haití**); alertas sobre virus incurables; falacias sobre personas, instituciones o empresas; cadenas de solidaridad; cadenas de la suerte; métodos para hacerse millonario; regalos de grandes compañías (véase el caso del bulo de Mercadona, por ejemplo) o mensajes de temática religiosa, entre otros.

Vishing

Una opinión de PaperBlog (Internet, 04/11/2011, 04/11/2011,14:07). "El usuario recibe un correo electrónico o mensaje SMS en el que se le dice que tiene que llamar a un número de teléfono para recibir una información, un regalo, o poder saber lo que alguien dice y/o piensa de él. Cuando el usuario llama al número en cuestión accede sin saberlo a un servicio que utiliza telefonía IP en el que se le pide información

personal (números de tarjetas o cuentas bancarias, usuarios o contraseñas de acceso, etc.) que se recopilaran y utilizaran para finalizar el timo.

2.4. Hipótesis

La implementación de la guía de seguridades influirá en la disminución del robo de la información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

2.5. Señalamiento de variables

VI: Guía de seguridades

VD: Robo de la información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Enfoque

El presente trabajo investigativo tomará un enfoque cuali-cuantitativo porque se basará en varios aspectos como son naturalista porque se mantendrá el entorno natural en el que se desarrollará la presente investigación, participativa porque van intervenir varias personas para la investigación de campo, etnográfica porque se realizará varias pruebas, normativo porque se realizará una guía de seguridades bajo ciertas reglas y normativas, y externa porque se realizará una encuesta a usuarios externos de la Cooperativa de Ahorro y Crédito 10 de Agosto.

3.2. Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad bibliográfica o documentada: se ha considerado esta modalidad porque se ha tomado información de libros, libros virtuales y tesis de grado.

Modalidad experimental: se ha considerado la relación de la variable independiente Guía de seguridades y su influencia y relación en la variable dependiente evitar robos de los fondos bancarios por medio del phishing para considerar sus causas y sus efectos.

Modalidad de campo: se ha considerado esta modalidad ya que el investigador ira a recoger la información primaria directamente de los involucrados a través de una encuesta.

3.3. Tipos de investigación

Se ha realizado la investigación exploratoria ya que permitió plantear el problema de la investigación robos de la información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto, de la misma manera ayudo a plantear la hipótesis: la implementación de la guía de seguridades evita el robo de la información mediante Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

Las unidades de observación son todos los empleados, clientes y jefe de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto.

También se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar el tiempo y el espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacionar ya que ha permitido medir la compatibilidad de la variable independiente guía de seguridades con la variable dependiente robo de la información por medio del phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

3.4. Población y muestra

La población considerada para la presente investigación son todas las personas que tengan cuenta en la Cooperativa de Ahorro y Crédito 10 de Agosto y el personal del departamento de Sistemas.

Cálculo de la muestra:

$$N = \frac{PQN}{(N-1)E^2/K^2 + PQ}$$

$$\text{n} = \frac{0{,}25(600)}{(600-1)0{,}1^2/2^2 + 0{,}25}$$

$$\text{n} = \frac{150}{(599)0{,}01/4 + 0{,}25}$$

$$\text{n} = \frac{150}{5.99/4 + 0{,}25}$$

$$\text{n} = \frac{150}{1.4975 + 0{,}25}$$

$$\text{n} = \frac{500}{5.24}$$

$$\text{n} = 95.42$$

$$n = 100$$

3.5. Operacionalización de variables

Hipótesis: La implementación de la guía de seguridades previene el robo de la información por medio del phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

Las unidades de observación son todos los empleados, clientes y jefe de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto.

Variable independiente: Guía de seguridades

Concepto	Categorías	Indicadores	Ítems	Técnicas e instrumentos
Es un conjunto de normas, reglas y procedimientos para la correcta navegación en el internet.	• Normas	• Niveles de seguridad al navegar en la web.	¿Qué seguridades toman los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto al momento de navegar en la web?	Encuesta a través de un cuestionario aplicado a los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto
		• Sitios más visitados	¿Qué páginas web son los más	Encuesta a través de un cuestionario aplicado a

			visitados por los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto?	los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto
	• Reglas	• Páginas web seguras	¿Pueden los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto identificar páginas web seguras?	Encuesta a través de un cuestionario aplicado a los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto
	• Navegación	• Mozilla • Explorer	¿Qué tipo de navegador utiliza la Cooperativa de Ahorro y Crédito 10 de Agosto?	Encuesta a través de un cuestionario aplicado al jefe del departamento de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto

	• Internet	• CNT • Portal Ambato	¿Qué proveedor de internet utiliza la Cooperativa de Ahorro y Crédito 10 de Agosto?	Encuesta a través de un cuestionario aplicado al jefe del departamento de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto.

Tabla2: Operacionalización de la variable independiente

Variable dependiente: Robo de la información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

Concepto	Categorías	Indicadores	Ítems	Técnicas e instrumentos
Consiste en el envío de correos electrónicos que, aparentando provenir de entidades formales **intentan obtener datos confidenciales del usuario.**	• Envió de Correos electrónicos	• Hotmail • Yahoo • Gmail	¿Poseen correos electrónicos los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto?	Encuesta con un cuestionario a los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto.
	• Datos confidenciales	• Información personal • Contraseñas • Cuentas bancarias	¿Qué tipo de información es más vulnerable a ser atacada en la Cooperativa de Ahorro y Crédito 10 de Agosto?	Encuesta con un cuestionario dirigido al jefe de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto
	• Páginas web	• Bancarias	¿Qué paginas son	Encuesta con un

	falsificadas	• Páginas de redes Sociales • Correos	las más falsificadas en internet?	cuestionario dirigido al jefe de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto

Tabla3: Operacionalización de la variable dependiente

3.6. Recolección y análisis de la información

TIPOS DE INVESTIGACIÓN

SECUNDARIA	PRIMARIA
• Se recolecta de estudios realizados anteriormente. • Se encuentra registrada en documentos y material impreso: libros, revistas especializadas, tesis de grado, etc. • Las fuentes de información son: bibliotecas, archivos, internet.	Se recolecta directamente a través del contacto directo entre el sujeto investigador y el objeto de estudio, es decir, con la realidad.

Tabla4: Tipos de investigación

TIPOS DE TECNICAS DE INVESTIGACIÓN

BIBLIOGRÁFICAS	DE CAMPO
• Análisis de documentos (lectura científica) • El fichaje	La encuesta

Tabla5: Tipos de técnicas de investigación

RECOLECCIÓN DE LA INFORMACIÓN

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis
2. ¿A qué personas o sujetos?	A los usuarios de entidades bancarias
3. ¿Sobre qué aspectos?	VI: Guía de seguridades

	VD: Robo de la información por medio del phishing.
4. ¿Quién?	Investigador: Patricio Analuiza
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de información?	Cooperativa de Ahorro y Crédito 10 de Agosto.
7. ¿Cuantas veces?	1 sola vez
8. ¿Qué técnica de recolección?	Encuesta
9. ¿Con que?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiana

Tabla6: Recolección de información

3.7. Procesamiento y análisis de la información

- **Revisión y codificación de la información**
- **Categorización y tabulación de la información**
  - Tabulación manual.
  - Tabulación computarizada.
- **Análisis de los datos**.
  - La presentación de los datos se dará atravesó de gráficos, cuadros para analizarlos e interpretarlo
- **Interpretación de los resultados.**
  - Describir los resultados.
  - Estudiar cada uno de los resultados por separado.
  - Redactar una síntesis general de los resultados.

CAPÍTULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis de la necesidad

Es necesario realizar una encuesta a los socios de la Cooperativa de Ahorro y Crédito 10 de Agosto para tener un conocimiento específico de cuáles son las deficiencias que los socios presentan al momento de navegar en el internet y de manera especial en la página web de la institución, además la encuesta permitirá saber si los socios tienen conocimiento sobre los peligros y delitos informáticos que existen en la web.

La encuesta también será aplicada al personal del departamento de sistemas, la cual permitirá conocer qué medidas de seguridad posee la página Web.

4.2. Análisis e interpretación de los resultados

Una vez que han sido tabulados los resultados obtenidos en la presente investigación se procede en este capítulo a organizar, analizar e interpretar los resultados. El procesamiento de los datos obtenidos, mediante la aplicación de los instrumentos de investigación se realizó utilizando una hoja electrónica en Excel 2007 la que nos

sirvió para la presentación de resultados en sus respectivos cuadros y gráficos estadísticos.

El análisis se realizó en forma literal y aplicando la estadística descriptiva. Los mismos que se presentan en cinco tablas organizados en filas y columnas que corresponden a las frecuencias y porcentajes de las categorías utilizadas en los ítems de los cuestionarios.

Para una mayor explicación de los resultados obtenidos y de la tabulación realizada se presenta gráficos que contienen los porcentajes de representación de las respuestas de la encuesta, lo cual nos ayudara a entender la situación de la cooperativa con respecto al problema planteado.

ENCUESTA REALIZADA A LOS SOCIOS DE LA COOPERATIVA

PREGUNTA 1

1. ¿Qué seguridades toma Ud. al momento de navegar en la página Web de la Cooperativa de Ahorro y Crédito 10 de Agosto?

N°	Indicador	Valores	%
1	Herramientas Informáticas	**20**	**20%**
2	Ayuda de un experto	**30**	**30%**
3	Ninguna	**50**	**50%**
	Total	**100**	**100%**

Tabla 7: Pregunta 1

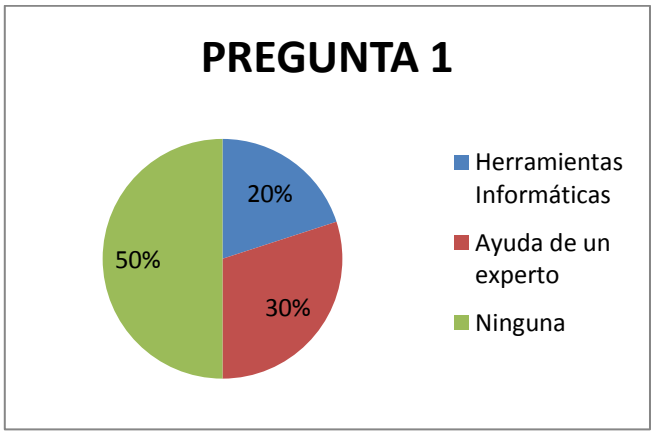


Figura 4: Seguridades de la página web

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 20 encuestados que representan el 20% indican que utilizan herramientas informáticas para las seguridades web, mientras que los 30 encuestados que representan el 30% dicen que piden ayuda de un experto y por otra parte de los 50 encuestados que representan el 50% mencionan que no toman ningún tipo de ayuda en cuanto a las seguridades en la web.

Cualitativo: La mayoría de los encuestados no toman ningún tipo seguridad al momento de navegar en la página web de la Cooperativa de Ahorro y Crédito 10 de agosto, por lo que ellos serían un blanco fácil para todos aquellos que gustan de robar la información personal por medio del Phishing, esto puede ocasionar múltiples inconvenientes para la cooperativa como para el socio, ya que puede existir robo de identidad, blanqueo de dinero, etc.

PREGUNTA 2

2. ¿Qué páginas web son los más visitados por Ud.?

N°	Indicador	Valores	%
1	Bancarias	**15**	**15%**
2	Descargas	**5**	**5%**
3	Videos	**30**	**30%**
4	Consultas	**20**	**20%**
5	Ninguna	**30**	**30%**
	Total	**100**	**100%**

Tabla 8: Pregunta 2

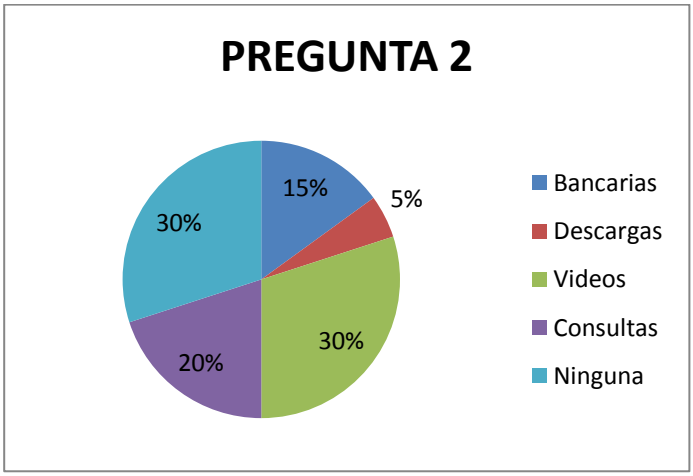


Figura 5: Páginas web más visitadas

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 15 encuestados que representan el 15% indican que visitan las páginas de entidades financieras, mientras que los 5 encuestados que representan el

5% dicen que navegan más en páginas de descargas, por otra parte de los 30 encuestados que representan el 30% mencionan que ingresan a las páginas de videos, también de los 20 encuestados que representan el 20% indican que utilizan las páginas de consultas o buscadores y de los 30 encuestados que representan el 30% mencionan que no utilizan el internet.

Cualitativo: La mayoría de socios de la Cooperativa de Ahorro y Crédito 10 de Agosto utilizan el internet ya sea para navegar en páginas de descarga, consultas, videos o de entidades financieras, lo que permite estar en peligro constante si no tomamos las medidas adecuadas para la navegación, debido a que en todas estas páginas estamos recibiendo constantemente anuncios publicitarios, mensajes sobre premios que hemos ganado, etc., estas páginas a lo único que con lleva es a ser uno más de las victimas del fraude informático llamado Phishing o (robo de información).

PREGUNTA 3

3. ¿Puede usted identificar páginas web seguras?

N°	Indicador	Valores	%
1	Si	**20**	**20%**
2	No	**80**	**80%**
	Total	**100**	**100%**

Tabla 9: Pregunta 3

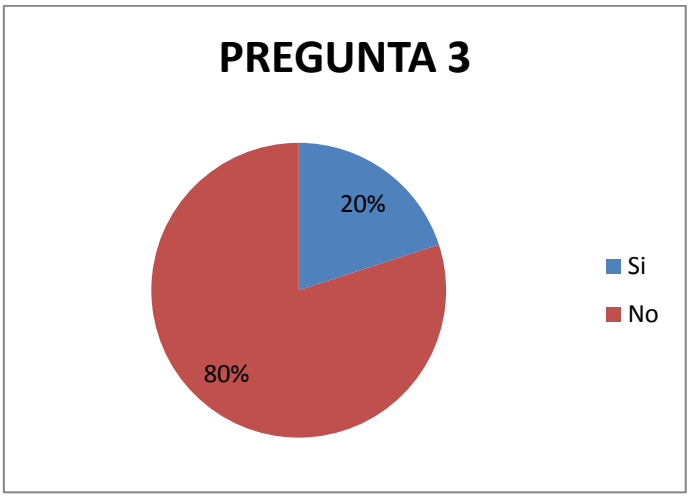


Figura 6: Identificación de páginas web seguras

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 20 encuestados que representan el 20% indican que si pueden identificar páginas web seguras pero de los 80 encuestados que representan el 80% dicen que no pueden identificar páginas web seguras.

Cualitativo: La mayoría de los socios encuestados indican que ellos no pueden identificar si una página de internet es segura o no porque ellos no tienen mucho conocimiento acerca de los peligros que existen en el internet peoraún las seguridades que se debería tomar al momento de navegar en estas páginas, por lo que estas personas no saben si han sufrido ya un robo de su información por medio el método del Phishing.

PREGUNTA 4

4. ¿Qué navegador utiliza al momento de entrar al internet?

N°	Indicador	Valores	%
1	Firefox Mozilla	50	50%
2	Internet Explorer	30	30%
3	Ninguna	20	20%
	Total	100	100%

Tabla 10: Pregunta 4

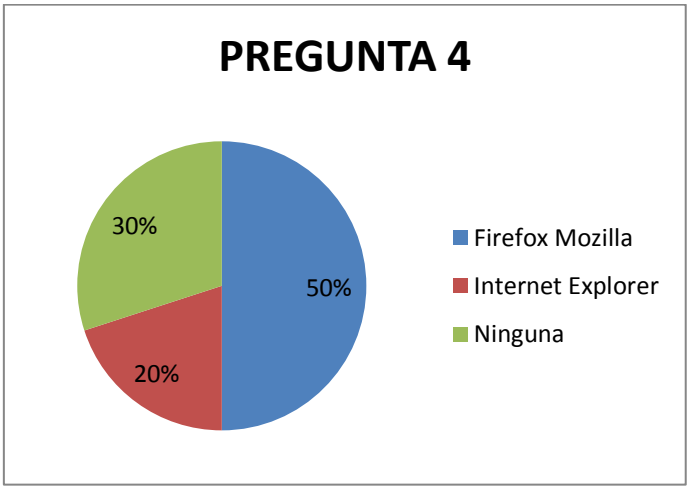


Figura 7: Navegadores de internet

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 50 encuestados que representan el 50% indican que utilizan como navegador FireFox Mozilla, mientras que los 20 encuestados que representan el 20% dicen que utilizan el internet Explorer y por otra parte de los 30 encuestados que representan el 30% mencionan que no utilizan ningún tipo de navegador.

Cualitativo: La mayoría de socios utilizan como navegador de internet a Firefox Mozilla el cual presenta un alto grado de vulnerabilidades ante amenazas de virus, suplantación de páginas web, etc., por lo tanto esta clase de socios no tienen seguridad al momento de navegar en sitios web, esto quiere decir que ellos podrían ser víctimas del robo de información; por otra parte el otro 20% de socios también

corren este peligro pero en menor proporción ya que el navegador de Internet Explorer posee mayores seguridades contra este tipo de amenazas.

PREGUNTA 5

5. ¿Qué tipo de servidor de correos utiliza usted en el internet?

N°	Indicador	Valores	%
1	Hotmail	**40**	**40%**
2	Gmail	**30**	**30%**
3	Yahoo	**20**	**20%**
	Ninguno	**10**	**10%**
	Total	**100**	**100%**

Tabla 11: Pregunta 5

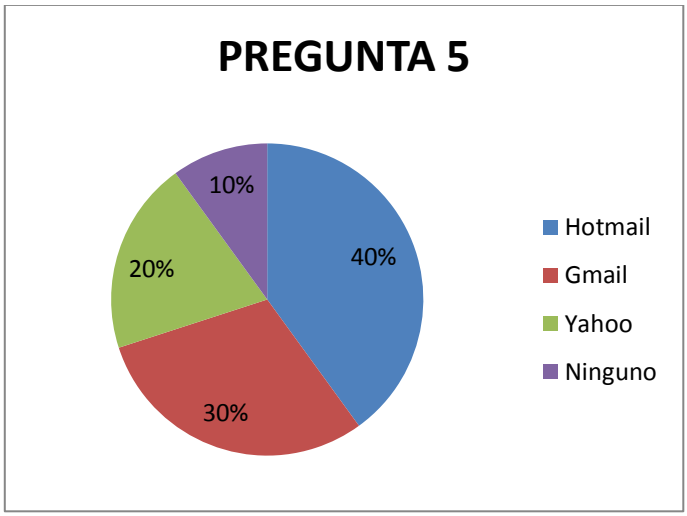


Figura 8: Servidor de correos

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 40 encuestados que representan el 40% indican que utilizan como correo electrónico el Hotmail, mientras que los 30 encuestados que representan el 30% dicen que utilizan el Gmail, por otra parte de los 20 encuestados que representan el 20% mencionan que utilizan el correo yahoo y por último de los 10 encuestados que representan el 10% dicen que no poseen cuentas en correos electrónicos.

Cualitativo: La gran parte de socios mencionan que el servidor de correos que utilizan es el de Hotmail, pero que quiere decir esto que según estadísticas y encuestas realizadas en Hotmail ingresan demasiados spam lo que quiere decir que es un peligro para aquellas personas que no conocen de los ataques informáticos; por otra parte también existen socios que utilizan el servidor de correos de Gmail, el cual filtra mejor lo que son spam pero tampoco podemos decir que estos socios se encuentra fuera de peligro pero si con menos riesgos.

ENCUESTA REALIZADA AL PERSONAL DE SISTEMAS

PREGUNTA 1

1. ¿Qué tipo de proveedor de internet utiliza la Cooperativa?

N°	Indicador	Valores	%
1	CNT	**3**	**100%**
2	El Portal	**0**	**0%**
3	Otros	**0**	**0%**
	Total	**3**	**100%**

Tabla 12: Tipos de proveedores

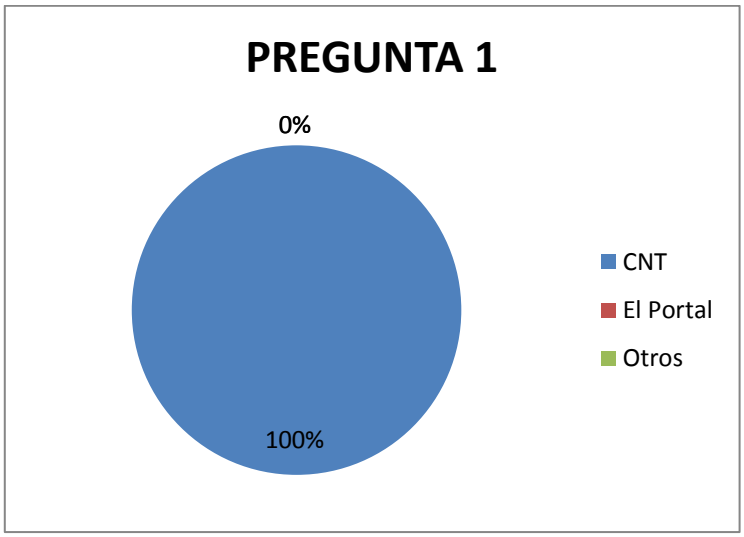


Figura 9: Proveedores de Internet

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 3encuestados que representan el 100% indican que utilizan como proveedor de internet los servicios de CNT.

Cualitativo: Las tres personas encargadas de administrar el departamento de sistemas mencionan que el proveedor del internet para la Cooperativa de Ahorro y Crédito 10 de Agosto es la empresa CNT, la cual es una de las empresas reconocidas del centro del país.

PREGUNTA 2

2. ¿Qué tipos de ataques lanzan los hackers a la Cooperativa?

N°	Indicador	Valores	%
1	Phishing	**2**	**67%**
2	Vishing	**0**	**0%**
3	Hoax	**0**	**0%**
4	Otros	**1**	**33%**
	Total	**3**	**100%**

Tabla 13: Tipos de ataques

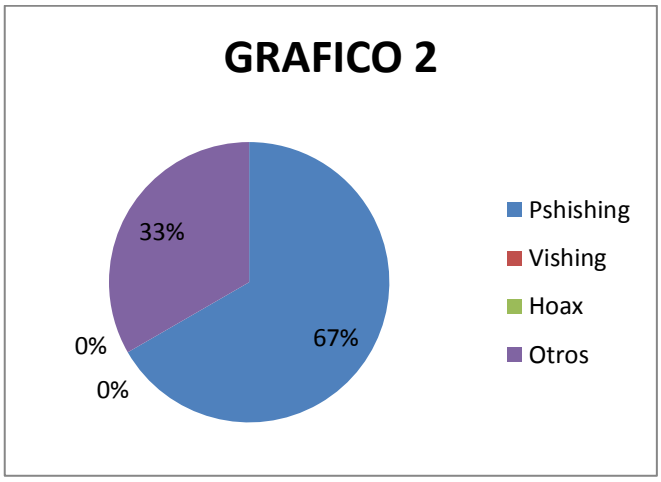


Figura 10: Ataques de Hackers

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: De los 2 encuestados que representan el 67% indican que los hackers utilizan mucho el ataque de Phishing que es él envió de correos electrónicos falsos, mientras que los la otra persona encuestada que representan el 33% dice que los hackers utilizan otros métodos para hacer daño a la Cooperativa.

Cualitativo: Dos personas mencionan que si existen en la Cooperativa de Ahorro y Crédito 10 de Agosto mensajes de correos fraudulentos que son enviados por personas que quieren obtener información confidencial, por otra parte mencionaron que existen otros medios para obtener información personal como por ejemplo llamadas anónimas.

PREGUNTA 3

3. ¿Qué tipo de información es más vulnerable a ser atacada en la Cooperativa?

N°	Indicador	Valores	%
1	Contraseñas	**1**	**33%**
2	Información Personal	**2**	**67%**
3	Cuentas	**0**	**0%**
	Total	**3**	**100%**

Tabla 14: Información vulnerable

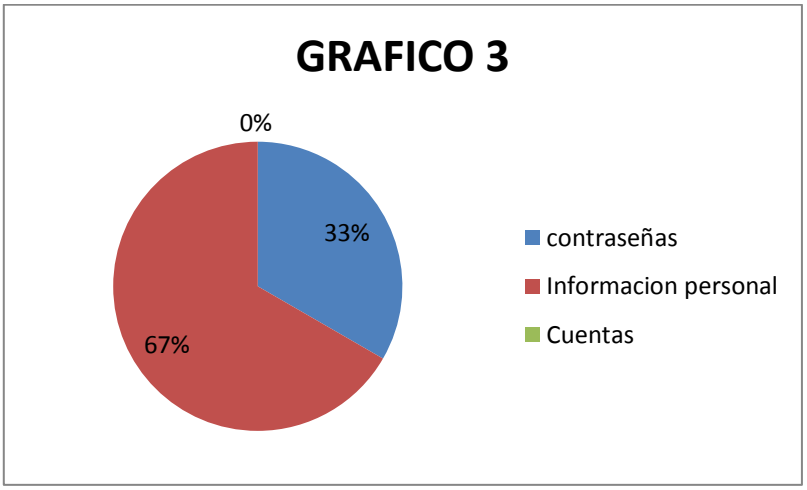


Figura 11: Vulnerabilidad de la información

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: Una de las personas encuestadas que representa el 33% indica que la información más propensa a ser robada es las contraseñas de los socios de la cooperativa, por otra parte 2 personas encuestadas que representan el 67% mencionan que la información personal de los socios es más vulnerable dentro de la Cooperativa.

Cualitativo: La mayor parte de las personas encuestadas indican que la información personal es más vulnerable dentro de la cooperativa porque en la página web la misma institución financiera pide que llene un formulario, esto hace que los phishers puedan duplicar el formulario y re direccionar a otro servidor y así obtener la información del socio.

PREGUNTA 4

4. ¿Qué paginas son las más falsificadas en internet?

N°	Indicador	Valores	%
1	Financieras	**1**	**33%**
2	Páginas de redes sociales	**0**	**0%**
3	Correos	**2**	**67%**
4	Otros	**0**	**0%**
	Total	**3**	**100%**

Tabla 15: Páginas web falsificadas

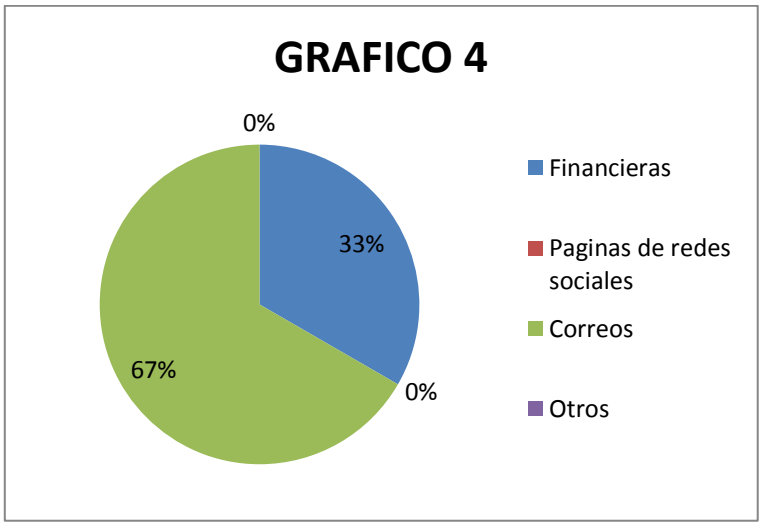


Figura 12: Páginas web falsificadas

Elaborado por: Patricio Analuiza

Fuente: Encuesta

ANÁLISIS:

Cuantitativo: Una de las personas encuestadas que representa el 33% menciona que las páginas que más falsifican o clonan los hackers son las páginas de entidades financieras, en cambio las dos personas encuestadas que representan el 67% indican que las páginas de internet que más falsifican son páginas de correos electrónicos.

Cualitativo: la mayor parte de las personas encuestadas indican que las páginas más falsificadas o fraudulentas son los correos electrónicos ya que por este medio de comunicación son como los phishers pueden obtener más fácilmente la información ya que con él envió de correos falsos el propio usuario puede estar dando información personal sin que este se dé cuenta.

4.2 Comprobación de la hipótesis

Se ha tomado en cuenta la **pregunta 1:**¿Qué seguridades toma Ud. al momento de navegar en la página de la Cooperativa de Ahorro y Crédito 10 de Agosto?, como pregunta discriminante de la encuesta aplicada, ya que los resultados arrojados , dicen que un alto porcentaje de socios de la Cooperativa 10 de Agosto no toman las medidas apropiadas de seguridad o en su defecto no saben de la existencia de seguridades para el internet al momento de revisar el movimiento de sus cuentas personales por lo cual podían ser fácilmente víctimas del fraude o robo de la información por medio del phishing.

También se tomó a la **pregunta 3:**¿Puede usted identificar páginas web seguras?, como la segunda pregunta discrimínate de la encuesta aplicada, debido a que los resultados que arrojó la encuesta dicen que la mayor parte de socios no puede identificar si una página web es o no falsificada o trae consigo algo que pueda afectar a la información de los usuarios

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Se puede determinar que se realiza actividades de tipo financiero y de consultas en la página oficial de la Cooperativa de Ahorro y Crédito 10 de Agosto, pero no se realiza un control de seguridades en la página Web, el cual debe estar orientado a estándares de creación de las páginas Webs de entidades financieras y a todos los métodos y procedimientos que están relacionados, principalmente con las seguridades que debe poseer la página Web de la Institución.

- La Cooperativa no tiene delimitado los parámetros o medidas de seguridad que se debe seguir al momento de ingresar a navegar en la página Web de la Cooperativa, por lo que se ha podido comprobar que la página web tiene muchas inseguridades y esto podría ocasionar robo de la información y por ende robos de identidades de los socios por los hackers.

- Las inseguridades que posee la página Web de la Cooperativa incide mucho en el robo de la información de los socios y de la Institución en sí, debido a que los socios y los empleados de la Cooperativa no cuentan con los conocimientos

suficientes acerca de los riesgos que se tiene al navegar en el Internet peor aún de los delitos informáticos que en este existen, por lo que los socios no poseen ninguna seguridad al momento de ingresar datos personales en la página Web de la Cooperativa de Ahorro y Crédito 10 de Agosto.

- En la Cooperativa 10 de Agosto no se posee un estudio o un registro de los ataques que se han realizado a la página Web de la Cooperativa, esto se da por la falta de conocimiento acerca de este tipo de ataques o delitos informáticos que afectan mucho a lo que es el sector financiero tanto de los socios como de la Cooperativa.

- Los socios de la Cooperativa de Ahorro y Crédito 10 de Agosto no cuentan con los conocimientos suficientes para poder prevenir o evitar los ataques de los diferentes Hackers que utilizan varias técnicas para poderse apoderas de nuestra información para luego cometer diferentes ilícitos.

5.2. Recomendaciones

- Con el fin de proteger la información de los socios y de la Institución por medio de estándares, métodos y procedimientos de las seguridades que debe tener una página Web financiera, se recomienda a los directivos de la Cooperativa de Ahorro y Crédito 10 de Agosto realizar el control de las seguridades en la página Web, con la finalidad que se reduzca el riesgo de robo o pérdida de la información de los socios.

- Para realizar una adecuada navegación en la página Web de la Cooperativa es necesario tener una guía de seguridades que permita identificar, analizar y prevenir un delito informático, evaluando de manera independiente cada uno de las diferentes formas de atacar con el método del Phishing,

- Se recomienda a la Institución efectuar capacitaciones acerca de los delitos informáticos existentes que tanto daño hacen a las instituciones financieras y a la estabilidad económica de un país, es por estas y varias razones que se propone a la Cooperativa de Ahorro y Crédito 10 de Agosto efectuar capacitaciones constantes a los socios acerca de los diferentes tipos de fraudes informáticos.

- La Cooperativa de Ahorro y Crédito 10 de Agosto deberá realizar un registro de los ataques que se han realizado a la página Web o a los cambios que terceros han realizado sin el consentimiento de los gerentes de la Institución.

- A la Cooperativa de Ahorro y Crédito 10 de Agosto se recomienda enfocarse más en los socios, para realizar un plan de capacitaciones acerca del método llamado Phishing, para que estos no sean víctimas del robo de la información, y así prevenir una serie de delitos que podrían efectuarse si los hackers obtienen información de los socios.

CAPÍTULO VI

6. PROPUESTA

6.1. Datos informativos

- **Titulo**

  Guía de seguridades para prevenir el robo de información por medio del Phishing en la Cooperativa de Ahorro y Crédito 10 de Agosto.

- **Institución ejecutora**

  Cooperativa de Ahorro y Crédito 10 de Agosto.

- **Director de tesis**

  Ing. ClayAldás

- **Beneficiario**

  Cooperativa de Ahorro y Crédito 10 de Agosto.

- **Ubicación**

  Av. 12 de Noviembre y Tomas Sevilla

- **Tiempo estimado para la ejecución**

  - Fecha de inicio: Enero de 2012
  - Fecha de finalización: Junio de 2012

- **Equipo técnico responsable**

  - Investigador: Patricio Analuiza
  - Gerente: Ing. Mary Hurtado
  - Coordinador: Ing. ClayAldás

6.2. Antecedentes de la propuesta

La Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato posee muchos tipos de inseguridades al momento de ingresar a la página Web de la Cooperativa por lo que los socios de la misma no se siente con las suficientes conocimiento acerca de las medidas de seguridad que se debe tomar al momento de navegar en la página de la Cooperativa por lo que tienen un poco de recelo de que su información ser robada y les puedan hacer cualquier tipo de daño informático.

Por tal motivo se establece que es beneficioso para la colectividad y socios de la Cooperativa la creación de una guía de seguridades la cual contenga medidas y reglas de seguridades que debemos seguir para la correcta manipulación e ingreso a la página oficial de la cooperativa.

6.3. Justificación

La guía de seguridades para prevenir el robo de la información en la Cooperativa de Ahorro y Crédito 10 de Agosto es un elemento de mucho interés para los clientes de la cooperativa, los aportes que la guía ofrece es netamente para tomar medidas de seguridad que los clientes de la cooperativa deben tomar al momento de navegar en la página oficial de la Cooperativa 10 de Agosto. Proteger la información de la institución y personal de los socios.

6.4. Objetivos

6.4.1. Objetivo General

Elaborar una guía de seguridades a través de un estudio del Phishing para prevenir los robos de información.

6.4.2. Objetivos Específicas

- Determinar las formas que se utilizan para navegar en la página oficial de la Cooperativa de Ahorro y Crédito 10 de Agosto.
- Establecer herramientas informáticas de seguridad para detectar páginas fraudulentas o correos maliciosos.
- Diseñar una guía de seguridades para prevenir el robo de información en la Cooperativa de Ahorro y Crédito 10 de Agosto.

6.5. Análisis de factibilidad

- **Político**

  Para la gerencia de la cooperativa se toma como política imprescindible la creación de una guía de seguridades para prevenir el robo de la información.

  La Cooperativa de Ahorro y Crédito 10 de Agosto tiene como política brindar las seguridades necesarias a todos sus clientes para la navegación segura en la página Web de la cooperativa.

- **Socio cultural**

  La puesta en marcha del proyecto ayudara a mejorar la navegación web de las personas socias de la Cooperativa de Ahorro y Crédito 10 de Agosto y por ente a la colectividad del centro del país, de esta manera la sociedad se verá afectada positivamente en razón de que se evitara un gran número de fraudes informáticos.

- **Tecnológico**

  El proyecto tiene como fin ayudar a mejorar las seguridades web en las diferentes tecnologías que día a día se va desarrollando para así no ser víctimas de los diferentes tipos de delitos informáticos.

- **Equilibrio de genero**

  El proyecto está desarrollado para que lo puedan aplicar tanto hombres como mujeres sin distinción de género porque la tecnología de estos días es para que lo use tanto hombres como mujeres.

- **Ambiental**

  El proyecto a desarrollar no atenta al medio ambiente puesto que es una guía de seguridades para el manejo de las páginas Web.

- **Económico - financiero**

  La Cooperativa de Ahorro y Crédito 10 de Agosto cuenta con los recursos económicos para financiar el proyecto, incluso para realizar capacitaciones a los socios acerca de este tipo de fraudes informáticos.

- **Legal**

  El proyecto se sujeta a las leyes y reglamentos de acuerdo a la ley que rige en el estado ecuatoriano y dentro de las normas establecidas en la Universidad Técnica de Ambato.

6.6. Informe técnico

6.6.1. Phishing

Phishing es una forma de estafa por Internet en donde los atacantes intentan convencer a los navegadores a divulgar información personal confidencial. Las técnicas para el robo de la información involucran e-mails y sitios Web fraudulentos que fingen ser e-mails y sitios Web legítimos. Los e-mails fraudulentos pueden ser considerados una forma malintencionada de e-mail en masa no solicitado más conocido como "spam." Los socios de las entidades financieras se quedan vulnerables al robo de identidades y a pérdidas financieras a través de transacciones fraudulentas. Las instituciones financieras están en riesgo debido al gran número de transacciones fraudulentas realizadas con la información robada. Los ataques de Phishing son eventos en gran escala cuyo blanco son miles de socios, esperando que una parte de ellos sea engañada. Los atacantes pueden copiar fácilmente imágenes, enlaces y textos de sitios Web legítimos para hacer que el e-mail parezca auténtico. Debido a la escala de los ataques, la posibilidad de ocurrir enormes pérdidas financieras es grande, estos involucran un millón o más de e-mails de Phishing.

Los objetivos más comunes son el robo de números de cuentas de tarjetas de crédito, débito y PIN. Toda persona que tenga algún tipo de cuenta en alguna entidad

financiera también vienen siendo los blancos de operaciones de robo de identidad.

6.6.2. Funcionamiento del Phishing

El ataque de Phishing empieza con el envío de un e-mail a las víctimas. El atacante crea el e-mail con el objetivo inicial de hacer que el destinatario crea que el e-mail pueda ser legítimo y que se debe aceptar. Las victimas aceptan el e-mail fraudulento y siguen las intrusiones que en el e-mail viene, finalmente las victimas reenvían el correo fraudulento con todos sus datos personales al phisher.

Pero ¿cómo obtienen los atacantes la direcciones de correo electrónico? Es una pregunta que la mayoría de personas se hacen, los atacantes obtienen direcciones de e-mail en diversas fuentes, incluso por generación semi aleatoria, buscándolos en fuentes en Internet y listas de direcciones que el usuario creía confidenciales.

Los servidores de correos electrónicos brindan alternativas para el filtrado de spam que puede bloquear muchos de los e-mails de Phishing.

6.6.3. Ataque a la Cooperativa 10 de Agosto

Para realizar un ataque que sea efectivo se creó un correo electrónico con el nombre de la Cooperativa 10 de Agosto, luego se realizó la creación de un e-mail con los logotipos de la Institución para que las victimas crean que es un correo legítimo, en el correo se les pide información personal como es: nombres, apellidos, dirección, teléfonos, Nueros de cedula, e incluso se les pide números de cuentas. Por último se realiza él envió del e-mail a 500 correos.

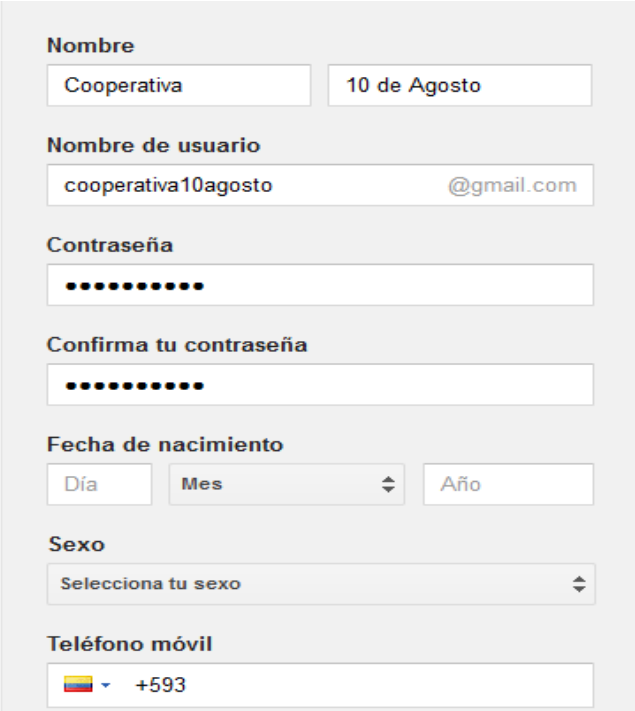


Figura 13: Creación de la cuenta

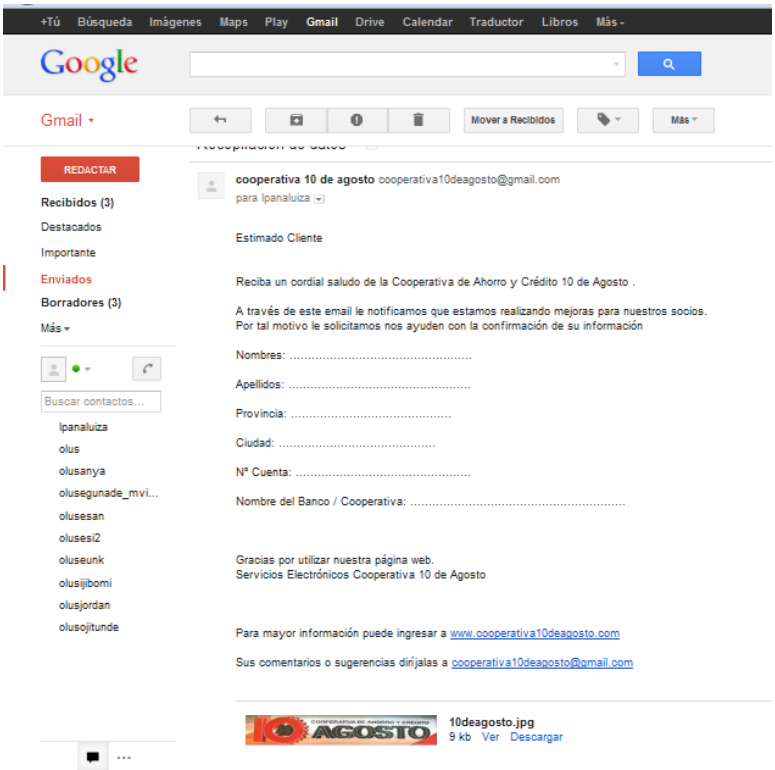


Figura 14: E-mail falso

Luego de varios días de espera comenzaron a llegar los correos con la confirmación de la información, es así como de los 500 correos electrónicos que se enviaron 35 correos fueron respondidos en donde se pudo observar que 20 correos fueron de mujeres y 15 fueron de hombres, lo que quiere decir que las mujeres son las más vulnerables para este tipo de ataques.

6.6.4. Estados de los ataques de Phishing

Los ataques de Phishing involucran diversos estados:

- El atacante obtiene las direcciones de e-mail de las víctimas, dichas direcciones pueden ser presumidas u obtenidas desde varias fuentes.
- El atacante genera un e-mail que parece legítimo y solicita que el destinatario realice alguna acción.
- El atacante envía el e-mail creado a sus víctimas de forma que parezca autentica y obscurezca la verdadera fuente.
- Dependiendo del contenido del e-mail, el destinatario abre un adjunto malicioso y llena un formulario o visita un sitio Web.
- El atacante recopila la información confidencial de la víctima y puede explotarlas en el futuro.

6.6.5. Fraudes que utilizan los atacantes para hacer caer a sus víctimas.

- Instalación de **Troyanos**, este método es la instalación de un software malicioso que no se comporta como espera el usuario.
- Utilización de **fraude**, este método trata de convencer al destinatario la continuación de algunas instrucciones.
- Utilización de **spyware,** El spyware es un programa que recopila secretamente información sobre las actividades del usuario (tecleo, sitios Web visitados, etc.), transmitiendo dicha información a terceros.

- Un **"bot"** es un tipo de programa malicioso que permite aun atacante tomar el control de un equipo infectado. Por lo general, los bots, también conocidos como "robots web" son parte deuna red de máquinas infectadas, conocidas como “botnet”, que comúnmente está compuesta por máquinas víctimas de todo el mundo.

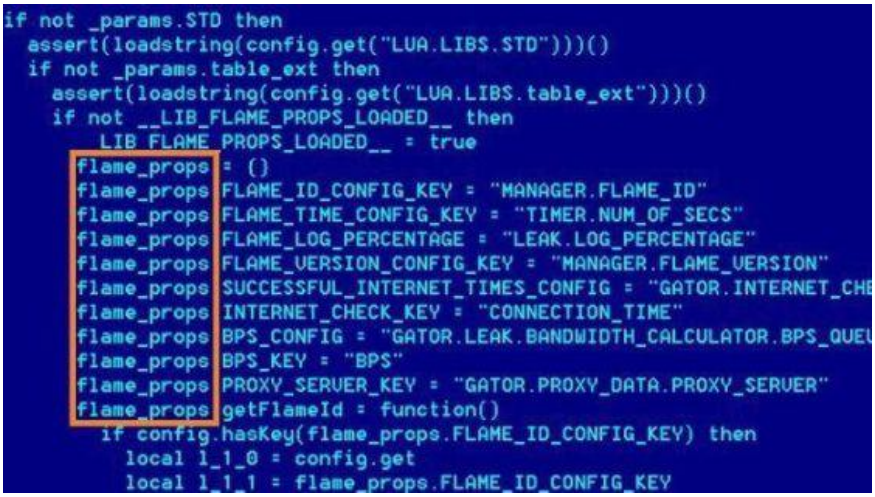
6.6.5.1. Troyanos

El atacante envía un adjunto de e-mail que finge ser bienintencionado, por ejemplo, una tarjeta virtual o un salvapantallas. En verdad el adjunto contiene un programa ejecutable que intercepta las comunicaciones posteriores entre la computadora de la víctima y una institución legítima. El programa espía transmite la información al atacante por la red.

SALVAPANTALLAS

Figura 15: Cooperativa de Ahorro y Crédito 10 de Agosto

CODIGO OCULTO EN EL SALVAPANTALLAS



```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
```

Figura 16: Código flame para ciberespiar

6.6.5.2. Fraude

El atacante utiliza la ley de los grandes números para asegurar que por lo menos algunos de los destinatarios se convenzan de que el e- mail es legítimo y sigan las instrucciones. El SSL (Secure Socket Layer) brinda alguna protección si el sitio Web del atacante lo utiliza, pero sólo si el destinatario está atento a los avisos del navegador sobre caracteres inválidos. Programas comerciales de protección de privacidad también pueden ser útiles, avisando al usuario cuando está en el momento de enviar información confidencial a destinos cuestionables.

Secure Socket Layer

Figura 17:Secure Socket Layer

6.6.5.3. Spyware

El atacante utiliza un programa espía previamente posicionado en la computadora de la víctima para extraer información confidencial. Esto se puede realizar a través de un ataque anterior por worm o Troyano, o por otros medios. A menudo, el spyware puede ser detectado por programas especializados en detección de spyware y por muchos antivirus disponibles comercialmente. Además, los firewalls personales y los sistemas de detección de intrusiones en el host pueden, a menudo, impedir que el spyware transmita información confidencial a terceros.

6.6.5.4. Botnet

Los bots se introducen sigilosamente en el equipo de una persona de muchas maneras. Los bots suelen propagarse por Internet en busca de equipos vulnerables y desprotegidos a los que puedan infectar. Cuando encuentran un equipo sin protección, lo infectan rápidamente e informan a su creador. Su objetivo es permanecer ocultos hasta que se les indique que realicen una tarea.

Los 10 programas espías más peligrosos

1. **CoolWebSearch (CWS):** Este programa toma el control del Explorer de manera que la página de inicio y las búsquedas del navegador se dirigen a los sitios web de quien controla el programa.
2. **Gator (o Gain):** Este programa en cambio abre ventanas de publicidad en el Explorer. Se aloja secretamente al instalar otras aplicaciones gratuitas.
3. **Internet Optimizer:** Este tipo de programa hace que sus autores se adueñan de las páginas de error del navegador que son las que aparecen cuando se trata de entrar a una dirección inexistente y las re direccionan a las que ellos controlan.
4. **PurityScan:** este programa espía promete borrar imágenes pornográficas que se encuentran en el disco duro cuando en realidad llena de ventanas publicitarias el navegador.
5. **n-CASE:** Este programa se instala secretamente con otras aplicaciones y abre numerosas ventanas emergentes cuando conoce los hábitos de navegación del usuario.
6. **Transponder o vx2:** Esta aplicación viene incluido en ciertas aplicaciones gratuitas, se incrusta en el Explorer para monitorear los sitios visitados y con ello conseguir información como los nombres de usuario y datos de formularios, esta información es empleada para enviar publicidad personalizada.
7. **ISTbar/AUpdate:** esta barra se instala en el Explorer supuestamente hace

búsquedas en sitios pornográficos, pero en realidad secuestra el navegador para direccionarlo a ciertas páginas web.

8. **KeenValue:** Este programa hace que se despliega ventanas emergentes publicitarias.
9. **Perfect Keylogger:** Esta aplicación audita y graba todos los sitios web visitados, las contraseñas y otra información que se escribe en el teclado, algo que claramente permite robar información confidencial del usuario.
10. **TIBS Dialer:** este marcador telefónico automático conecta la computadora, sin que el usuario se dé cuenta, con sitios y servicios pornográficos que no son gratuitos.

6.6.6. Recomendaciones para la Cooperativa de Ahorro y Crédito 10 de Agosto

- **Establecer políticas corporativas y divulgarlas a los socios:** Cree políticas corporativas de contenido de e-mail para que no se puedan confundir los mensajes legítimos con phishing. Divulgar dichas políticas a los socios y realizar un seguimiento.

- **Crear una manera para que el socio confirme si el e-mail es legítimo:** El socio debe ser capaz de identificar si el e-mail proviene de la Cooperativa de Ahorro y Crédito 10 de Agosto y no de un phisher. Para eso la Cooperativa de Ahorro y Crédito 10 de Agosto necesita establecer una política para incluir información de autenticación en todos los e-mails enviados por ella a los socios.
- **Autenticación más rígida en los sitios Web:** Si la Cooperativa de Ahorro y Crédito 10 de Agosto no solicita información confidencial de los socios para la entrada en el sitio Web de la Cooperativa, por ejemplo números de documentos o contraseñas es más difícil para que los phishers extraigan dicha información del socio.
- **Monitorear el Internet en busca de sitios Web que puedan ser de phishing:** Generalmente, el sitio Web de phishing aparece en algún lugar de Internet antes

del envío de los e-mails de phishing. Dichos sitios Web se apropian indebidamente de marcas comerciales de empresas o entidades financieras para que parezcan legítimos.

- **Implementar soluciones de antivirus, de filtrado de contenido y anti-spam de buena calidad en el punto de contacto (gateway) con Internet:** La exploración antivirus en el gateway establece una capa de defensa más allá de la exploración antivirus en la propia máquina. Filtre y bloquee sitios Web de Phishing conocidos en el gateway. El filtrado de spam en el gateway ayuda a los usuarios finales a evitar mensajes no deseados y e-mails de Phishing.

6.6.7. Recomendaciones para los Socios de la Cooperativa

- **Bloquee automáticamente mensajes malintencionados o fraudulentos:** Los detectores de spam pueden ayudar a evitar que el socio tenga que abrir e-mails sospechosos.
- **Detecte y excluya automáticamente los programas malintencionados:** Los programas espías son parte de un ataque de Phishing, pero pueden ser eliminados por muchos programas disponibles en el mercado.
- **Bloquee automáticamente la salida de información confidencial a terceros:** Aunque el socio no logre identificar visualmente el verdadero sitio Web que recibirá la información confidencial, existen productos de software que lo logran.
- **Siempre desconfíe:** Si usted no está seguro de que un e-mail es legítimo, llame a la Cooperativa que envió el e-mail para verificar su autenticidad.

Ninguna de dichas soluciones constituye, individualmente, una respuesta completa al problema. Se recomienda una combinación de contramedidas que:

- Reducirá el número de ataques de Phishing enviados a los socios;

- Aumentará la probabilidad de que el socio reconozca un ataque de Phishing;
- Reducirá las oportunidades de que el socio provea inadvertidamente información confidencial.

6.6.8. Medidas preventivas para la Cooperativa 10 de Agosto

6.6.8.1. Evitar hiperenlaces incorporados

Problema

Los e-mails comerciales legítimos poseen hiperenlaces al sitio Web de la Cooperativa, que solicitan que el socio envíe información confidencial, incluso el nombre del usuario y la contraseña. Los phishers aprovechan dichos enlaces incorporados para llevar a los consumidores a revelar dicha información a sitios Web fraudulentos.

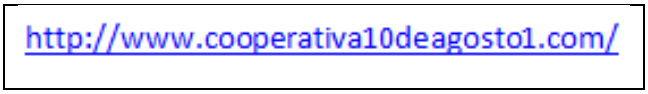


Figura 18: Hiperenlace falso

Solución

Una alternativa más segura es incluir en el e-mail un enlace no pulsable donde el socio tenga que teclear o cortar y pegar en el navegador. Muy probablemente, los socios regulares tendrán el enlace de la Cooperativa en su lista de sitios preferidos, facilitando aún más dicho proceso.

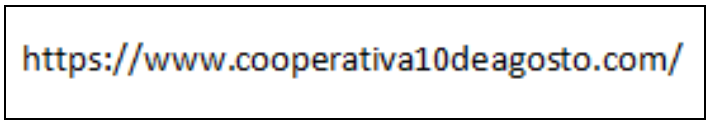


Figura 19: Hiperenlace verdadero

Ventajas

- El número de ataques de Phishing a través de URL engañosas puede ser reducido.
- La Cooperativa y socios no necesitaran instalar nuevos programas en sus computadoras.

Desventajas

- La navegación del socio será negativamente afectada, aunque muy poco.
- Quizás algunos grupos e individuos de la Cooperativa no siempre sigan la política, llevando a la falta de uniformidad y a la confusión entre los socios.
- Quizás no siempre los socios sigan las políticas implementadas por la Cooperativa, por lo que pueden seguir siendo engañados por e-mails fraudulentos con hiperenlaces incorporados.

Recomendación

La Cooperativa debe evaluar con cuidado el impacto sobre la comodidad para el socio respecto al aumento de la seguridad que brinda la implementación de esta política. Esto puede ser adecuado para muchas instituciones financieras.

6.6.8.2. Evite formularios de e-mail

Problema

Los phishers utilizan formularios de e-mail para recolectar información personal de los socios. Como la Cooperativa también utiliza dichos formularios, será difícil para el socio distinguir entre e- mails legítimos y fraudulentos.

Figura 20: Formulario

Solución

La Cooperativa deberá informar a los socios de que los e-mails legítimos nunca contendrán formularios solicitando información personal.

Ventaja

- Los ataques de Phishing a través de formularios de e-mail pueden ser reducidos.

Desventajas

- La comodidad para el socio será ligeramente afectada.
- Los consumidores que reciben e-mails fraudulentos, pero que no son socios de la Cooperativa, pueden no estar al tanto de la política implementada por la Cooperativa.

Recomendación

La Cooperativa de Ahorro y Crédito 10 de Agosto deberá estar muy pendiente de todos los e-mails enviados a sus socios para llevar un control y así mejorar las seguridades en el envió de correos con formularios.

6.6.8.3. E-mails firmados digitalmente

Problema

Los socios no cuentan con un medio infalible para verificar la autenticidad de los mensajes potencialmente importantes provenientes de instituciones legítimas.

Solución

La Cooperativa de Ahorro y Crédito 10 de Agosto debe establecer una política por la cual todas las comunicaciones de alto valor por e- mail con los socios sean digitalmente firmadas con una clave privada autorizada. Al recibir el e-mail, el destinatario verifica la autenticidad a través de la clave pública de la institución. Existe una probabilidad muy pequeña de que un phisher logre crear una firma válida para un e-mail fraudulento.

Figura 21: Firmas digitales

Ventajas

- Las firmas digitales son extremamente difíciles de falsificar.
- Los mensajes pueden ser verificados automáticamente por lectores de e-mail.

Desventajas

- Es poco probable que el socio instale y mantenga una tecnología de firma digital.
- Los que no son clientes de la institución no conocerán la política de la Cooperativa de firmar todos los e-mails.

Recomendación

Para un pequeño número de cuentas de socios con transacciones de alto valor, esta solución vale la consideración.

6.6.8.4.Personalización visual o sonora de e-mails

Problema

El cliente común no cuenta con un medio sencillo de verificar la autenticidad de los mensajes provenientes de instituciones legítimas.

Solución

Esta solución pretende crear un mecanismo visual o sonoro para verificar la autenticidad de los e-mails. La cooperativa podría incluir una fotografía del socio en todas las comunicaciones electrónicas. Este es un método sencillo y confiable para que el socio de la Cooperativa reconozca los mensajes legítimos sin que necesite precisar instalar ningún software más en su máquina. Los socios deficientes visuales utilizarían un objeto de identificación alterno quizás una "imagen sonora" o una palabra de acceso adjuntado adecuadamente.

Ventajas

- El cliente final no necesita ningún software o hardware más.
- Los mensajes pueden ser fácilmente verificados por los socios sin conocimientos sofisticados.
- El valor de las tarjetas de crédito "personalizadas" ya establecido en el mercado; se puede asociar fácilmente con dicho mensaje de marketing.
- Reduce la probabilidad de ataques en gran escala, pues los phishers necesitan recopilar mensajes anteriores de la institución para cada cliente para obtener la información de personalización.

Desventajas

- Gastos considerables de marketing para divulgar el mensaje "No acepte mensajes que no contienen su fotografía".
- Aumento considerable del costo de generación de los mensajes.
- Los socios necesitan comparecer en persona a la Cooperativa para que se saque su fotografía.
- La Cooperativa debe proteger rígidamente la base de datos que contiene los datos de autenticación (fotos, clips de sonido o contraseñas).
- El método no es completamente a prueba de fraude, pero eleva el nivel de seguridad.

Recomendación

Para ciertas instituciones, especialmente las que emiten tarjetas de crédito, esta puede ser una solución viable si ya capturan imágenes digitales para tarjetas de crédito u otras finalidades.

6.6.8.5. Numeración secuencial de e-mails

Problema

El cliente común no cuenta con un medio simple de verificar la autenticidad de los mensajes provenientes de instituciones legítimas.

Solución

Se trata de incorporar el equivalente a una numeración secuencial a cada e-mail

enviado por la Cooperativa. Los números de secuencia serían una forma previsible de autenticación que el socio podría verificar fácilmente. Ejemplo:

Fecha: 16 de enero de 2010
Número de Serie: JJH0017

El último e-mail que le enviamos fue el JJH0016 el 10 de diciembre de 2010.
El próximo e-mail que le enviaremos tendrá el número de serie JJH0018

Ventajas

- El socio no necesita ningún software o hardware más.
- Reduce la probabilidad de ataques en gran escala, pues los estafadores necesitan recopilar mensajes anteriores de la Cooperativa para cada socio para obtener la información de personalización.

Desventajas

- Un poco más de dificultad de confirmación por el socio debido a la necesidad de mantener el e-mail más reciente.
- Quizás los socios no verifiquen los números de secuencia.
- Aumento considerable en el costo de generación de los mensajes.
- La Cooperativa necesita proteger de manera estricta la base de datos que contiene los números de secuencia.

Recomendación

Si no es posible obtener imágenes digitales o información semejante de personalización, esta es la segunda solución más confiable. Sin embargo,

también es la más propensa a fallos para un gran número de socios.

6.6.8.6. Incorporación del nombre del socio al e-mail

Problema

El socio no cuenta con un medio sencillo de verificar la autenticidad de los mensajes de la Cooperativa.

Solución

Es simplemente incorporar el nombre del socio al e-mail, por ejemplo, "Estimado Sr. Jones".

Ventajas

- Los mensajes pueden ser fácilmente verificados por socios que no poseen un conocimiento avanzado sobre estos tipos de ataques.
- Reduce la probabilidad de un ataque exitoso en larga escala, pues los phishers necesitan recopilar o suponer la información de personalización de muchos socios.

Desventajas

- No siempre los socios percibirán que falta su nombre en el e-mail.
- La Cooperativa debe proteger de manera rígida la base de datos que contiene los datos de autenticación.

Recomendación

Todas las instituciones deben emplear esta solución. Si esta es la política que predomina en todas las instituciones financieras, los socios podrán acostumbrarse a esperar la presencia de su nombre en los e- mails.

6.6.8.7.Monitoreo activo de la Web

Problema

El contenido de Web presente en e-mails de Phishing es obtenido desde fuentes legítimas, con URL dirigidas a fuentes ilegítimas.

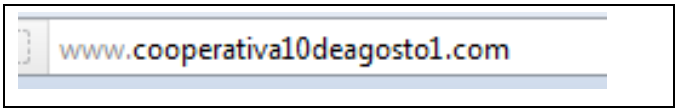


Figura 22: URL Falso

Solución

Las empresas de servicios de monitoreo implementan soluciones que utilizan agentes para monitorear continuamente el contenido de la Web, buscando activamente todas las instancias del logotipo de un cliente, de su marca comercial o de su contenido-clave de Web. La institución cliente presenta a la empresa proveedora del servicio de monitoreo una “lista blanca” de usuarios autorizados del logotipo, de la marca comercial y del contenido clave. Cuando los agentes detectan usuarios no autorizados de logotipos, marcas comerciales u otros contenidos de la Web, la institución cliente puede tomar medidas de resolución.

Figura 23: URL verdadero

Ventajas

- Los propietarios de contenido son alertados respecto a posibles usuarios clandestinos de contenido reservado.
- Órdenes de "cese y desista" son generadas como resultado del monitoreo activo de contenido y de la identificación de uso inadecuado.
- Las reglas de filtrado de spam pueden ser rápidamente actualizadas por los proveedores para bloquear e-mails que contengan referencias a sitios Web malintencionados.

Desventajas

- Exigencia del monitoreo activo.
- El desfase entre la identificación y la acción de eliminación de uso puede asimismo resultar en varios robos de información particular.

Recomendación

Se debe tomar en cuenta esta técnica como parte de un paquete de iniciativas de reducción del impacto económico de las amenazas de Phishing.

6.6.9. Medidas preventivas para los socios de la Cooperativa de Ahorro y Crédito 10 de Agosto

6.6.9.1. Filtrado anti-spam en la computadora

Problema

No siempre los socios logran detectar los e-mails fraudulentos que aparentemente provienen de la Cooperativa.

Solución

El filtrado anti-spam puede bloquear algunos e-mails fraudulentos antes de que logren alcanzar al consumidor. Los e-mails de Phishing son una forma específica de spam. El socio debe instalar un software en la computadora y configurarlo.

Ventajas

- Los e-mails fraudulentos pueden ser bloqueados antes que el socio de la cooperativa pueda contestarlos, bloqueando el ataque en su estado inicial.
- Existen varios tipos de software que realizan estos bloqueos.

Desventaja

- Las soluciones anti-spam para PC exigen que el socios de la Cooperativa compre, instale y mantenga el software.
- Debido a las grandes variaciones de técnicas utilizadas por los atacantes los socios pueden no implementar la tecnología de manera eficaz.

Recomendación

Los socios deben pensar en comprar y usar productos de filtrado de spam para así estar mejor protegido y no ser un blanco fácil para este tipo de ataque.

6.6.9.2.Direcciones de Internet

Problema

Falsificación de direcciones de Internet y técnicas de Phishing

Solución

La nueva protección contra el fraude financiero y el robo de identidad, ha sido incorporado un filtro contra falsificaciones, que aparece en el menú de opciones de Internet, y que tiene la intención de proteger a los usuarios contra la divulgación de información privada, a terceros no autorizados, sin el correspondiente consentimiento.

Si un usuario visita un sitio falso, que parece exactamente igual que el original, por lo general después de pulsar sobre un enlace en un correo electrónico fraudulento, el navegador detecta un intento de falsificación de dirección y compara el sitio con una lista de sitios conocidos de falsificación de direcciones.

Si el filtro detecta que el sitio es culpable de falsificar la dirección, bloquea el acceso al mismo e informa al usuario del peligro de dejar su información personal en sitios como ese.

La base de datos de sitios conocidos con direcciones falsificadas, se actualiza de forma regular y los usuarios tienen la opción de informar una instancia sospechosa de falsificación a Microsoft, para una evaluación.

Ventajas

- Detecta automáticamente páginas Web falsas.
- Ayuda al socio a proteger la información personal.
- No tiene ningún costo para el socio.
- Estos filtros permiten informar a una base de datos de Microsoft sobre paginas falsificadas.

Desventajas

- Siempre debe estar actualizado la base de datos de las páginas Web falsas.

6.6.9.3.Software Antivirus y Anti-spyware

Problema

Los programas espías interceptan invisiblemente las comunicaciones entre el socio y las instituciones financieras.

Solución

Los programas antivirus detectan muchas formas de programas malintencionados, incluso el spyware pudiendo excluirlo cuando se lo encuentre. La mayoría de los programas antivirus funciona de manera casi invisible para el usuario, afectando poco a sus operaciones normales. Los programas anti-spyware pueden explorar la computadora en busca de posibles programas espías y son capaces de eliminarlos.

Figura 24: Antivirus y Anti - Spyware

Ventajas

- Detecta y excluye el spyware antes de que logre interceptar información confidencial.
- Mayor seguridad al momento de realizar cualquier actividad en nuestro computador.

Desventajas

- La detección es según el tipo de antivirus.
- El software anti-spyware puede eliminar algunos programas espías necesarios para la operación correcta de programas legítimos
- El socio debe comprar e instalar el software.

Recomendación

Los socios deben instalar programas antivirus, con opciones activadas para detectar programas potencialmente indeseables. Los socios de la cooperativa también deben

mantener sus programas antivirus actualizados.

6.6.9.4.Servicio de privacidad de desktops

Problema

Los socios pueden ser inducidos a enviar datos confidenciales a sitios Web inseguros y fraudulentos.

Solución

Existe software que puede monitorear el tráfico de la Web saliente respecto a un conjunto de datos que el usuario puede definir. Los datos definidos con mayor frecuencia son información que identifican al usuario, tales como nombre, Apellido y números de tarjetas de crédito. Si se encuentra cualquiera de dichos conjuntos de datos en uno de los paquetes enviados, el paquete se queda retenido hasta que el usuario confirme si los datos deben ser enviados al destino verdadero, o si se debe interrumpir la transmisión de los datos. Si el usuario indica que los datos no deben ser enviados, los datos confidenciales son eliminados del paquete

Figura 25: Software de monitoreo de tráfico en la web

Ventajas

- Este tipo de software logra ver si el destinatario es una entidad legítima o fraudulenta.
- Protegemos nuestra información confidencial de mejor manera.

Desventaja

- Exige la instalación de software en la computadora del socio de la cooperativa.

Recomendación

Los socios de la Cooperativa deben adoptar este tipo de medida para mejorar y proteger sus datos confidenciales y así poder observar si al destinatario que enviamos nuestra información es legítima o no.

6.6.9.5. Teclear las direcciones de la Web y verificar su autenticidad

Problema

Varias exploraciones pueden ocultar la verdadera dirección de Web de un enlace y redirigir el navegador a un sitio Web de Phishing.

Solución

Es más seguro teclear en el navegador la dirección de Web deseada que pulsar en enlaces incorporados. Si usted no está seguro sobre la autenticidad de un e-mail, contacte directamente con la institución remitente.

Figura 26: Dirección Web

Ventaja

- Mayor seguridad al momento de ingresar a una página web.

Desventajas

- Direcciones de Web largas y propensas a errores.
- Puede ser difícil verificar algunos e-mails.

Recomendación

Conozca la política de Cooperativa respecto a la solicitud de información personal confidencial. En caso de duda, consulte a la institución por teléfono o a través de un e-mail que usted conozca.

CAPÍTULO VII

7. CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

- El fraude informático Phishing es uno de los métodos más utilizados por los grandes hackers porque es un método de Ingeniería Social donde se utiliza el ingenio para hacer caer a las personas en el fraude.
- El método del Phishing es muy común aplicar en entidades financieras debido a que la mayoría de estas entidades utilizan páginas Web donde piden información personal al socio como son: nombres, apellidos, número de cuentas, contraseñas, etc., por ende los atacantes prefieren este tipo de páginas porque son más fáciles de acceder a la información.
- La guía permitirá educar tecnológicamente a las personas a una mejor navegación por la Web debido a que en la guía muestra indicaciones que deben seguir tanto la Institución financiera como es la Cooperativa de Ahorro y Crédito 10 de Agosto y sus socios.
- El Phishing a igual que es muy funcional también posee muchas vulnerabilidades como se demuestra en la guía de seguridades las cuales pueden

ser muy útil para todos los socios de la Cooperativa de Ahorro y Crédito 10 de Agosto, siempre y cuando lo pongan en práctica.

7.2. Recomendaciones

- Se recomienda a la Cooperativa de Ahorro y Crédito 10 de Agosto adoptar algunas medidas de seguridad para prevenir el robo de información por medio del Phishing, las cuales se indican en la guía de seguridad.
- Es necesario que la Cooperativa de Ahorro y Crédito 10 de Agosto brinde capacitaciones a los socios para que de esta manera los socios tengan conocimiento de las medidas de seguridad que deben tomar al momento de navegar en la Web.
- Los socios de la Cooperativa de Ahorro y Crédito 10 de Agosto podrán prevenir el robo de información por medio del Phishing siempre y cuando pongan en práctica todo lo indicado en la guía de seguridades.
- La Cooperativa de Ahorro y Crédito 10 de Agosto deberá brindar todas las medidas de seguridad a sus socios, para que de esta manera puedan navegar en una página Web segura y confiable de la Institución.
- Se recomienda a la Institución utilizar la guía de usuarios para prevenir el robo de la información, para que de esta manera los socios no cometan la imprudencia de entregar la información personal a terceras personas.

GLOSARIO DE TERMINOS

Blog

Versión reducida del término "web log". Es información que un usuario publica de forma fácil e instantánea en un sitio web. Generalmente un blog se lee en orden cronológico.

Buscador

Los buscadores (o motor de búsqueda) son aquellos que están diseñados para facilitar encontrar otros sitios o páginas Web. Existen dos tipos de buscadores, los spiders (o arañas) como Google y los directorios, como Yahoo.

Ciberespacio

El conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el cual casi todo lo que contiene es información.

Cibernética

Término acuñado por un grupo de científicos dirigidos por Norbert Wiener y popularizado por su libro "Cyberneticsor Control and Communication in the Animal and the Machine" de 1948.

Firewall.- Literalmente " Muro de Fuego". Se trata de cualquier programa que protege a una red de otra red. El firewall da acceso a una maquina en una **red local** a Internet pero Internet no ve más allá del firewall. Un firewall es una utulidad o herramienta de seguridad que impide que ciertos comandos o paquetes de datos "anormales" penetren a nuestro sistema, detectan ataques o entradas forzadas en los puertos de nuestro sistema.

Click

Cuando se oprime alguno de los botones de un mouse el sonido es parecido a un "click". La palabra click escrita, se usa generalmente para indicarle al usuario que oprima el botón del mouse encima de un área de la pantalla. También es comúnmente

escrito así: clic. En español incluso se usa como un verbo, por ejemplo: al clickear en el enlace.

Freeware.- Programas de dominio público, programas de libre distribución, programas gratuitos. Programas informáticos que se distribuyen a través de la red de forma gratuita.

IP.- Internet Protocol. **Protocolo** de Internet. Bajo este se agrupan los protocolos de internet. También se refiere a las direcciones de red Internet.

Password.- Palabra de paso, contraseña. Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado. Palabra clave.

PING.- PacketINternetGroper. Rastreador de Paquetes Internet. Programa utilizado para comprobar si un **Host** está disponible. Envía paquetes de control para comprobar si el host está activo y los devuelve.

Spam/Spammer.- Se llama así al "bombardeo" con correo electrónico, es decir, mandar grandes cantidades de correo o mensajes muy largos.

TCP.- Transmission Control Protocol. Protocolo de control de Transmisión. Uno de los protocolos más usados en Internet. Es un protocolo de TransportLayer.

TCP/IP.- Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

Cliente

Aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. Sistema o proceso el cual le solicita a otro sistema o proceso la prestación de un servicio.

Contraseña

Password. Código utilizado para accesar un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

Cracker

Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio.

Criptografía

Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

Directorio web

Las páginas que se incluyen en la base de datos del directorio son previamente revisadas por humanos (no es automatizado como los crawlers o arañas). No se agrega la página completa, sino únicamente algunos datos tales como el título, la URL y un breve comentario redactado especialmente que explique el contenido, y se la ubica en una categoría. Un ejemplo es www.yahoo.com

Download

Descarga. Proceso en el cual información es transferida desde un servidor a una computadora personal.

e-mail

El e-mail o email, del inglés electronic mail (correo electrónico), ha sido uno de los medios de comunicación de más rápido crecimiento en la historia de la humanidad. Por medio del protocolo de comunicación TCP/IP, permite el intercambio de mensajes entre las personas conectadas a la red de manera similar al correo tradicional.

Firefox

Mozilla Firefox (originalmente conocido como Phoenix y Mozilla Firebird) es un navegador de web gráfico, gratuito, de código abierto, desarrollado por la Fundación Mozilla y miles de colaboradores en el mundo. La versión 1.0 salió el 9 de noviembre de 2004. Instalable en los sistemas operativos Windows, Linux i686 y Mac Os X.

Hoax

Término utilizado para definir a los falsos rumores, especialmente sobre virus inexistentes difundidos por la red, y hay veces que tienen mucho éxito y causan casi tanto daño como si se tratase de un virus real. Recomendamos revisar cualquier historia que te llegue por email antes de reenviarla, en Snopes.com.

Hotmail

Uno de los más populares sitios que otorgan cuentas de email gratis (@hotmail.com), cuenta con millones de usuarios a nivel mundial. Fue comprado por MSN Networks, empresa miembro del grupo Microsoft.

Internet

Una red mundial, de redes de computadoras. Es una interconexión de redes grandes y chicas alrededor del mundo.

Internet2

Proyecto que trata de crear una nueva Internet de mayores y mejores prestaciones en el ámbito de las universidades norteamericanas.

Mail

Programa en ambiente UNIX para la edición lectura y respuesta de emails.

Phishing

"Phishing" (pronunciado como "fishing", "pescar" en inglés) se refiere a comunicaciones fraudulentas diseñadas para inducir a los consumidores a divulgar información personal, financiera o sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, entre otros.

Virus

Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas.

BIBLIOGRAFÍA

Páginas de internet

- PaperBlog. (2011). Diferentes tipos de phishing. 4 de Octubre del 2011. Disponible en: http://es.paperblog.com/diferentes-tipos-dephishing-timos-en-la-red-81585/2011

- Segu-info. (2011). Estafa nigeriana. 7 de Octubre del 2011. Disponible en: http://www.a1hosting.com.pe/blog/estafas/la-estafa-nigeriana-explicacion-en-detalle/

- El Universo, (2011). Desarrollo Tecnológico. 7 de Octubre del 2011. Disponible en: http://www.eluniverso.com/2008/04/09/0001/9/F6818ADB15634D6C9D15993CDF479F90

- Bits Cloud, (2011). Fraudes bancarios en el Ecuador. 5 de Octubre del 2011. Disponible en: http://bitscloud.com/2011/04/el-fraudebancario-en-ecuador-un-tema-en-auge/,2011

- Taringa. (2011). Cómo evitar el phishing. 28 de Septiembre del 2011. Disponible en: http://www.taringa.net/posts/taringa/9949868/Comoevitar-el-phishing-roba-cuentas.html,2011

- Slideshare.net. (2011). Robos y fraudes informáticos. día 28 de Octubre del 2011. Disponible en:

http://www.slideshare.net/guest0b9717/robos-yfraudes-informticos-presentation,2011

- Gonzalo Alvarez. (2011). Las profundidades del phishing, 28 de Septiembre del 2011. Disponible en: http://www.iec.csic.es/gonzalo/descargas/phishing.pdf,2011

- Panda Security. (2011). Tipos de amenazas. 6 de Octubre del 2011. Disponible en: http://www.pandasecurity.com/spain/enterprise/securityinfo/types-malware/phishing/,2011

- Segu-info. (2012). Que es el hoax. 12 de Marzo del 2012. Disponible en: http://www.segu-info.com.ar/malware/hoax.htm

- Antivirus. (2012). Hoax. 12 de Marzo del 2012. Disponible en: http://www.vsantivirus.com/hoaxes.htm

- Wordpress. (2012). Cartas nigerianas. 18 de Marzo del 2012. Disponible en: http://inza.wordpress.com/2007/05/05/cartas-nigerianas-spam-y-scam/

- Wikipedia. (2012). Vishing. 18 de Marzo del 2012. Disponible en: http://es.wikipedia.org/wiki/Vishing

- Infosecwriters. (2012). Guía de vishing. 20 de Mazo del 2012. Disponible en:

http://www.google.com.ec/url?sa=t&rct=j&q=vishing&source=web&cd=9&ved=0CHkQFjAI&url=http%3A%2F%2Fwww.infosecwriters.com%2Ftext_resources%2Fpdf%2FIBM_ISS_vishing_guide_GOllmann.pdf&ei=WopNT9-QG8_egQfnjPWiAg&usg=AFQjCNGRkzA_73E5o24sATf5fQRr1cljFw&cad=rja

- Fbi. (2012). News. 20 de Marzo del 2012. Disponible en:

  http://www.fbi.gov/news/stories/2010/november/cyber_112410

- Anónimo. (2012). Vishing. 20 de Marzo del 2012. Disponible en:

  http://idtheft.about.com/od/glossary/g/Vishing.htm

- Finextra. (2012). Phishing. 20 de Marzo del 2012. Disponible en:

  http://www.finextra.com/community/fullblog.aspx?id=4791

- Wikipedia. (2012). Esquema de pirámide. 20 de Marzo del 2012. Disponible en:

  http://es.wikipedia.org/wiki/Esquema_de_pir%C3%A1mide

- Practicopedia. (2012). Que es una estafa piramidal. 20 de Marzo del 2012. Disponible en:

  http://www.practicopedia.com/inversion/que-es-una-estafa-piramidal-1165

- Invertirenbolsa. (2012). Cómo funciona la estafa piramidal. 20 de Marzo del 2012. Disponible en:

http://www.invertirenbolsa.info/articulo_como_funcionan_estafas_piramidales.htm

- Wordpress. (2012). Estafas piramidales. 20 de Marzo del 2012. Disponible en: http://gua30.wordpress.com/2008/01/13/herbalife-%C2%BFestafa-piramidal/

- Laflecha. (2012). Estafas piramidales. 25 de Marzo del 2012. Disponible en: http://www.laflecha.net/canales/curiosidades/noticias/como-funcionan-las-estafas-piramidales

- Anonimo. (2012). Antiphishing. 25 de Marzo del 2012. Disponible en: www.nai.cl/es/partners/literature/wp_antiphishing_Inst&cons_es.pdf

ANEXOS

ANEXO 1
Fórmula de cálculo de la muestra

$$n = \frac{PQN}{(N-1)E^2/K^2 + PQ}$$

n: Tamaño de la muestra

Pq: Constante de varianza de población (0.25)

N: Tamaño de la población

E: Error máximo admisible (al 1%=0.01 al 10%=0.1)

K: Coeficiente de error (2)

ANEXO 2
Croquis de la Cooperativa 10 de Agosto

ANEXO 3

Encuesta para los clientes de la Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISITEMAS, ELECTRÓNICA E INDUSTRIAL

CIUDAD DE AMBATO

OBJETIVO DE LA ENCUESTA

La encuesta tiene como objetivo observar que tipos seguridades utilizan los clientes de Cooperativa al momento de navegar en la Web.

Señores, su veracidad en las respuestas permitirá al grupo investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva de su información.

Cuestionario

1. ¿Qué seguridades toma Ud. al momento de navegar en la página de la Cooperativa de Ahorro y Crédito 10de Agosto?

☐ Herramientas Informáticas
☐ Ayuda de un experto
☐ Otros

2. ¿Qué páginas web son los más visitados por Ud.?

☐ Financieras
☐ Descargas
☐ Videos

- ☐ Consultas
- ☐ Otros

3. ¿Puede usted identificar páginas web seguras?

- ☐ Si
- ☐ No

4. ¿Qué navegador utiliza al momento de entrar al internet?

- ☐ Firefox Mozilla
- ☐ Internet Explorer
- ☐ Otros

5. ¿Qué tipo de servidor de correos utiliza usted para en el internet?

- ☐ Hotmail
- ☐ Gmail
- ☐ Yahoo
- ☐ Otros

Gracias por su colaboración.

Fecha de aplicación:

ANEXO 4

4.2.1. Encuesta para el departamento de sistemas de la Cooperativa de Ahorro y Crédito 10 de Agosto de la ciudad de Ambato

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISITEMAS, ELECTRÓNICA E INDUSTRIAL

CIUDAD DE AMBATO

OBJETIVO DE LA ENCUESTA

La encuesta tiene como objetivo analizar las seguridades que posee la Cooperativa para brindar el servicio web a sus clientes.

Señores, su veracidad en las respuestas permitirá al grupo investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva de su información.

Cuestionario

1. ¿Qué tipo de proveedor de internet utiliza la Cooperativa?
   - ☐ CNT
   - ☐ El Portal
   - ☐ Otros

2. ¿Qué tipos de ataques lanzan los hackers a la Cooperativa?
   - ☐ Phishing
   - ☐ Vishing
   - ☐ Hoax
   - ☐ Otros

3. ¿Qué tipo de información es más vulnerable a ser atacada en Cooperativa?
   - ☐ Contraseñas
   - ☐ Información Personal
   - ☐ Cuentas

4. ¿Qué paginas son las más falsificadas en internet?

   - ☐ Financieras
   - ☐ Páginas de redes Sociales
   - ☐ Correos
   - ☐ Otros

Gracias por su colaboración.

Fecha de aplicación: