PROYECTO DE GRADO

"PHISHING: LA AUTOMATIZACIÓN DE LA INGENIERÍA SOCIAL"

POR:

NATALIA SALAZAR

200110008081

MARCELA GONZÁLEZ

200210033010

ASESOR:

JUAN GUILLERMO LALINDE

ESCUELA DE INGENIERÍA

INGENIERÍA DE SISTEMAS

UNIVERSIDAD EAFIT

MEDELLLÍN

2007

DESARROLLADORES

Marcela González Arango

Cód. 200210033010

Email: mgonza16@eafit.edu.co

Tel: 3124445

Cel: 300-3653971

Natalia Andrea Salazar Aristizábal

Cód. 200110008081

Email: nsalaza2@eafit.edu.co

Tel: 5484350

Cel: 300-6013596

ASESOR

Juan Guillermo Lalinde Pulido

Profesor Departamento de Informática y Sistemas

Coordinador Maestría en Ingeniería Informática

Email: jlalinde@eafit.edu.co

Tel: 2619596 ext: 282

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del jurado

_____
Firma del jurado

Medellín, Octubre de 2007

TABLA DE CONTENIDO

1. RESUMEN

El presente trabajo contiene una recopilación de la información que presentan algunos bancos tanto nacionales como internacionales con respecto a Seguridad informática más concretamente “Ingeniería social: Phishing”, un tema que tiene gran auge en la actualidad por la incidencia en la red y las consecuencias negativas que ha presentado sobre los usuarios de los diferentes entidades financieras.

Finalmente se presentan a los usuarios del Internet unos tips generales de cómo evitar este tipo de fraudes.

2. INTRODUCCION

Desde el principio de los tiempos, el ser humano ha evolucionado radicalmente cambiando su estilo de vida. Las personas tomamos decisiones basados en las experiencias cotidianas y, en algunos casos, sólo se hace uso de la intuición.

El hombre se ha visto influenciado por un sin número de cosas que lo han hecho evolucionar y hacer cosas como las que vemos hoy día. Para lograr la creación de éstas, tuvo que saber manejar lo que comúnmente conocemos con el nombre de Información. "La información es un fenómeno que proporciona significado o sentido a las cosas, e indica mediante códigos y conjuntos de datos, los modelos del pensamiento humano. La información por tanto, procesa y genera el conocimiento humano"[1]; por lo que si no se manipula de una manera adecuada no se logran los objetivos propuestos.

Es común que los seres humanos busquemos a otros para lograr algún fin común. Es ahí entonces, donde el uso adecuado de la información toma importancia, ya que con el conocimiento humano puesto en marcha es que los inventos han cobrado vida.

Uno de los mayores inventos en el campo de la tecnología, y que partió la historia del hombre en dos, es la del Internet. A partir del momento en el cual ésta se abrió al mundo entero, la forma de hacerse las cosas cambiaron. Por ejemplo, antes de la aparición de Internet, todas las tareas del colegio se hacían buscando en una enciclopedia y se sacaba de allí toda la información que se necesitaba. Ahora con solo dar un clic, se obtiene la información deseada; pueden ser noticias, biografías, y muchas otras cosas. También es importante tener en cuenta, que Internet no solo se usa para informarse sino que también para realizar cualquier tipo de diligencia. Realizar el mercado, pagar la universidad, subscribirse en una revista, etc. son algunos ejemplos de lo que el maravilloso mundo del Internet permite hacer.

A simple vista, Internet parece ser la "última maravilla del desierto" y todo en su uso pareciera "perfecto", pero la realidad es otra. Como todo en la vida, está el lado bueno y malo de las cosas. En este caso el lado "malo" de Internet, por llamarlo de alguna manera, es la seguridad. Se debe tener cuidado con la forma como los niños usan la herramienta ya que también se encuentra contenido no apto para menores de edad como lo es el contenido sexual explícito, apología al suicidio, etc. Adicionalmente hay problemas de gran dimensión como la pornografía infantil, la cual, pese a ser ilegal en la gran mayoría de los países, ha florecido en este medio.

---

[1] http://es.wikipedia.org/wiki/informaci%c3%b3n

En el tema de comercio en línea, está la principal preocupación con todo lo relacionado a seguridad. Es vital, porque a la hora de realizar cualquier tipo de transacción financiera vía Internet, como por ejemplo una compra, es necesario del uso de la tarjeta de crédito u otro medio de pago electrónico para cerrar la transacción. Entonces la seguridad que se le brinda al cibernauta, es la que garantiza que éste use de nuevo el servicio por Internet o no; ya que si hay violación o hurto de su información personal éste no recurrirá de nuevo a Internet.

"Actualmente, el tema del hurto en Internet está muy de moda, ya que éste es el medio más rápido y sencillo que los ladrones tienen para realizar robos con una probabilidad muy baja de que sean descubiertos"[2].

En este punto, se introducen entonces, dos términos. El primero hace referencia a la manipulación de las personas mediante técnicas de persuasión, también conocidas actualmente como "*Ingeniería social*". Éste es importante que sea mencionado, ya que con su uso las personas han sido víctimas de ataques de hurto de información personal. Y el segundo término, es una aplicación específica de la Ingeniería social y es una de las palabras más sonada del momento "El phishing". Ésta es una modalidad de robo que surgió gracias a la buena acogida que ha tenido el comercio electrónico actualmente. El phishing consiste, en el hurto de la información personal de alguien, mientras que éste navega en Internet sin que se dé por enterado. Éste proceso de robo lo realizan los ladrones o "phishers" en el ciberespacio.

El fraude mediante el uso del correo electrónico, hace parte de la modalidad de phishing. Éste consiste en que el atacante envía un correo electrónico a su víctima, solicitándole que ingrese datos personales como: cédula, número de cuenta, tarjeta de crédito, entre otros. Entonces el usuario, sin darse cuenta de que la fuente del correo no es autentica, realiza el ingreso de datos dando clic sobre un link que lo lleva a una página de Internet que ha sido diseñada de manera que el usuario crea que la conoce y que aparentemente es segura. El problema se da, porque en realidad esta página es una imitación del sitio original, o sea que allí el usuario está siendo víctima de phishing sin saber.

El gran reto que existe hoy en día tanto para los navegantes de Internet como para los programadores es la seguridad. Por lo tanto, hay que informarse más de lo que está ocurriendo a nuestro alrededor y así conocer que es lo que los crackers o hackers están planeando desarrollar para poder contrarrestar sus efectos.

---

[2] http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/s-transcript_library.pdf

3. FORMULACIÓN DEL PROBLEMA

3.1. JUSTIFICACIÓN

Cada día son más comunes los ataques informáticos basados en la *Ingeniería Social*[3]. Estos se caracterizan por explotar la confianza de los usuarios con el fin de tener acceso a información confidencial. Entre ellos se destaca el phishing, el cual consiste en orientar al usuario para que ingrese a una página falsa, generalmente asociada con una entidad financiera, y obtener información privilegiada.

Con base en las experiencias relatadas por los usuarios acerca del impacto que tiene la "*Ingeniería Social",* se hace necesario definir unas estrategias de contingencia mediante el profundo conocimiento de las políticas de seguridad que manejan las organizaciones, con el fin de evitar el constante fraude al que los usuarios son expuestos día a día.

Una de las perspectivas para atacar el problema es definir algunos criterios básicos que le permitan al usuario de Internet diferenciar sitios auténticos de sitios falsos.

Este proyecto ataca la perspectiva descrita anteriormente, utilizando como ejemplos particulares sitios hipotéticos de instituciones financieras.

3.2. OBJETIVOS

3.2.1. GENERALES

Documentar estrategias, de navegación, que permitan a los usuarios de Internet detectar cuando son víctimas de ataques de phishing, con el fin de evitar captura de información.

3.2.2. ESPECIFICOS

- Establecer estrategias preventivas y correctivas que permitan al cibernauta navegar de una forma segura.
- Definir estrategias, basados en las políticas de seguridad de la organización, que permitan a los usuarios del sitio verificar fácilmente que la página a la que están conectados es autentica.

3.3. IMPORTANCIA EN LA CARRERA Y EN EL MEDIO

[3] http://www.terra.com.mx/tecnologia/articulo/113507/

Debido al incremento en el uso del Internet durante estos últimos años para realizar transacciones virtuales, se debe garantizar a los usuarios seguridad a la hora de realizar estas tareas para que aumente el uso del comercio electrónico y la consulta en los diferentes sitios Web.

La temática que se desarrollará está estrechamente relacionada con la carrera de Ingeniería de Sistemas ofrecida por la Universidad EAFIT, especialmente con el área de seguridad informática, ya que se pretende responder a la carencia de información que tienen los usuarios, concretamente para aquellos directamente relacionados con entidades bancarias.

4. METODOLOGIA

Para la elaboración del presente trabajo seguimos la siguiente metodología:

1. Recolección de la información.

2. Análisis de la Información recolectada.

3. Análisis de la Información existente en la Web a cerca de las entidades financieras nacionales e internacionales.

4. Analizar algunos casos concretos de Phishing en Colombia.

5. De acuerdo a los anteriores puntos se realizó un análisis de los principales aspectos que deben tener los usuarios de la red.

6. Elaboración de los tips a tener en cuenta a la hora de realizar transacciones online.

5. ESTADO DEL ARTE

En estos últimos años las personas se han concienciado de lo importante que es la seguridad informática. En Colombia, las transacciones por Internet han crecido y por esto, las empresas financieras están luchando por prestar un servicio en línea a sus usuarios de manera más segura. Debido a los diferentes incidentes que se están presentando diariamente como, el robo de información, desfalcos financieros, suplantación de identidad entre otros tipos de incidentes; es que las medidas preventivas también han crecido.

A continuación se pretende dar la respuesta a los siguientes interrogantes: ¿Que es el phishing? ¿Cual fue su origen?, ¿Cual ha sido su evolución? y ¿Como esta el phishing hoy en día?

Origen de la palabra

Como es mencionado en los textos bibliográficos *"La palabra Phishing proviene de la palabra en ingles "fishing" (pesca)*[4]*".* Si nos detenemos a pensar un poco, podremos afirmar que la palabra pesca es utiliza ya que el phishing es una pesca de información que realizan los hackers en Internet para poder robar información a los cibernautas de sus cuentas bancarias.

Haciendo la comparación entre la pesca en general y el phishing, encontramos que en la pesca se usa una carnada para poner en el anzuelo y con esta atrapar los pescados. En el phishing también se usa una carnada y se pone en un anzuelo. Para este caso el anzuelo sería la bandeja de entrada de los correos electrónicos de los cibernautas y la carnada sería un e-mail enviado aparentemente por una entidad financiera. Así entonces, las personas al revisar sus cuentas de correo y encontrar un e-mail de alguna entidad financiera donde ellos tienen cuenta, "*morderían*" el anzuelo y revelarían su información personal.

Historia del Phishing

"*La primera mención del término phishing data de enero de 1996 en un grupo de noticias de hackers alt.2600*[5]*, aunque el término apareció tempranamente en la edición impresa del boletín de noticias hacker "2600*

---

[4] spam slayer: do you speak spam? pcworld.com. [3]. 16 de agosto del 2006.

[5] "phish, v." oed online, march 2006, oxford university press. oxford english dictionary online. http://dictionary.oed.com/cgi/entry/30004303/ 9 de agosto de 2006.

Magazine"[6]. El término phishing fue adoptado por crackers que intentaban "pescar" cuentas de miembros de AOL".

Las personas que se dedican al phishing son conocidas con el nombre de phishers[7](pescadores). Estos individuos tienen como función principal el envío de correos electrónicos a diferentes personas. Para poder lograr que las personas crean que el correo que reciben es de un remitente confiable, los phishers deben de hacerse pasar por entidades financieras[8] que sean reconocidas en el medio.

Los ataques de phishing están creciendo con gran rapidez y por esta razón es que se ha hecho necesario tomar medidas de seguridad contra estos ataques. Existen leyes en la actualidad que penalizan esta modalidad de robo. Por otra parte se han encontrado nuevas variantes para realizar el phishing, como lo es[9] el robo de información por medio del teléfono.

Evolución del Phishing

Como se mencionó anteriormente, el inicio del Phishing se dio al ser mencionado por primera vez en un grupo de noticias de hackers. Entonces desde esa época fue que se dio el nacimiento de la nueva modalidad de robo, también conocida como phishing.

El primer intento de phishing, como también se mencionó, se dio cuando un grupo de ckrackers querían robar algunas cuentas de miembros de AOL. Después de eso, es muy difícil decir un número exacto de casos reportados por personas que hayan sido víctimas de phishing.

Existen dos clases de phishing, el tradicional y el complejo. El primero es aquel que se envía de manera masiva a los diferentes buzones de correo electrónico de personas escogidas al azar. Lo anterior hace que el detectar estos correos se pueda realizar de manera más rápida. Por otro lado, esta clase de phishing tiene elementos muy visibles que hacen que las personas sepan identificar cuando los correos son fraudulentos o no.

Actualmente en el mundo entero existen entidades y empresas que son conocidas y que tienen la facilidad de identificar cuando un sitio Web es o no auténticos. Con base en la información anterior, se afirma que estos

---

[6] ollmann, gunter. phishing guide: understanding and preventing phishing attacks. technical info. [4]. 10 de julio del 2006.

[7] stutz, michael aol: a cracker's paradise? 29 de enero de 1998.

[8] tan, koon. phishing and spamming via im (spim). internet storm center. [1]. 5 de diciembre del 2006.

[9] [2]. ed skoudis. phone phishing: the role of voip in phishing attacks. 13 de junio del 2006.

incidentes no trascienden; además se tiene que los ataques mostrados en estadísticas nunca serán los reales.

Entre las medidas preventivas, a las personas que navegan en Internet se les da una serie de indicaciones como no dar su información personal en correos electrónicos que les llegue a sus bandejas de entrada; dentro de ésta información personal están las contraseñas, usuarios, números de tarjetas de crédito, entre otras. Por otro lado, los usuarios deberán estar alerta cuando entren a sitios Web de entidades financieras y cerciorarse de la existencia de dos detalles muy importantes, el primero es fijarse si la dirección o URL esta antecedida por una *´s´* que indica que es página segura, así: http**s**://. Y lo segundo a tener en cuenta es verificar la existencia de un candado en la parte inferior derecha de sus pantallas, el cual advierte que la página es segura.

Toda la información descrita anteriormente demuestra que el la clase de phishing tradicional es una forma un poco primitiva pero que igual es peligrosa y es de suma importancia para la seguridad de los cibernautas. En la actualidad no hay cifras reales de pérdida monetaria a causa del phishing ni del número de personas afectadas por esta modalidad. Lo anterior también muestra que esta actividad es muy rentable para los phishers adquirir dinero de manera "fácil"[10].

Por otro lado hay que mirar éste problema de phishing desde el punto de vista no del usuario, sino de las diferentes entidades bancarias a las cuales les plagian sus páginas en Internet para robar dinero. A pesar de ser éste otro contexto, las consecuencias son iguales o peor de devastadoras. Para una empresa y más para una entidad financiera, lo primordial es conservar el *good will* y si tomamos aquellos casos en los que los phishers lograron su acometida será ahí donde la buena imagen de las empresas decaería.

"El problema del phishing no acaba aquí, y por ende es necesario evolucionar en la forma de abordarlo, ya que en la actualidad no se está llevando a cabo de forma efectiva, hay muchas áreas de oportunidad desaprovechadas"[11].

Haciendo alusión a la parte técnica que esta relacionada con éste tema del phishing, es fundamental mencionar que para que los ataques de phishers disminuyan notoriamente es necesario combatir directamente con el talón de Aquiles de éste tema, el cual es la integridad del sistema del usuario.

Dentro del tema de seguridad, las empresas desarrolladoras de antivirus juegan un papel muy importante, ya que estas cuentan con personal capacitado técnicamente y un software de seguridad que está muy bien

---

10 http://www.elpelao.com/3831.html

11 http://ip-com.blogspot.com/2006_07_01_archive.html

probado y la implantación del mismo ha sido exitosa. A pesar de lo anterior estas empresas no se libran de los ataques de phishing.

Por otro lado hay que tener en cuenta que el sistema operativo del navegador tiene mucho que ver a la hora de hablar de phishing. Esto se debe a que los hackers constantemente están documentándose e informándose para crear ataques más potentes y así encuentran debilidades o vulnerabilidades del software que se puedan explotar[12].

Ataques recientes

En general, los últimos ataques de phishing han sido reportados desde páginas de Internet habilitadas para realizar pagos y por clientes de entidades financieras. También se ha encontrado que últimamente páginas de carácter social han sido víctimas de ataques de phishing debido al gran contenido de información personal de diferentes personas que frecuentan el sitio[13]. "*Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques*"[14].

Un ejemplo muy peculiar se dio a finales del año 2006, en el cual un gusano informático tomo posesión de varias de las páginas de MySpace, un sitio muy conocido y de gran concurrencia. Los phishers lograron hacer que los enlaces de éste sitio Web se dirigieran a otra página diferente pero con una apariencia igual o muy similar a la original[15].

Lavado de dinero producto del phishing

Otra forma de realizar el phishing indirectamente siendo *mula*. Este término se le da aquella persona que participa en los ataques de phishing muchas veces sin tener conocimiento. Un ejemplo de esto y que se ha dado a conocer en estos días, es el del sinnúmero de ofertas que a diario vemos por ahí solicitando personas para trabajar desde la comodidad de su casa. Para poder ser contratado en este tipo de trabajos es necesario llenar un formulario en el cual piden varios datos personales, entre ellos números de

---

12 http://www.laflecha.net/canales/seguridad/200607131/

13 http://www.pcworld.com/resource/article/0,aid,125956,pg,1,rss,rss,00.asp/ phishing scam takes aim at myspace.com. jeremy kirk. idg network. 2 de junio del 2006 (en inglés).

14 tom jagatic and nathan johnson and markus jakobsson and filippo menczer. social phishing. a publicarse en communications of the acm. 3 de junio del 2006. (en inglés).

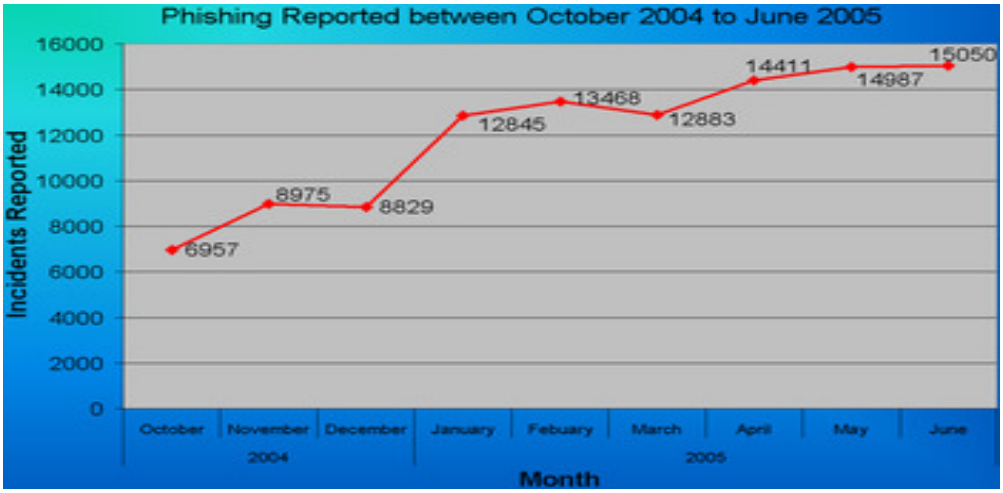
15 malicious website / malicious code: myspace xss quicktime worm. websense security labs. 5 de diciembre del 2006.

cuentas bancarias; con esta información es que los phishers se basan para realizar sus ataques.

Éstos lo que hacen, es consignar la plata obtenida en alguno de sus ataques en las cuentas de estos "*trabajadores*" y así en caso de ser descubiertos no podrán ser encontrados por el número de cuenta. Los empleados de dicha empresa recibirán un porcentaje del dinero obtenido en el fraude como parte de pago por su trabajo.

Algunos daños causados por el phishing

A continuación se muestra una gráfica que expone el crecimiento acelerado de ataques de phishing desde Octubre del 2004 hasta Junio del 2005.



"Se estima que entre mayo del 2004 y mayo del 2005, aproximadamente 1.2 millones de usuarios de computadoras en los Estados Unidos tuvieron pérdidas a causa del phishing, lo que suma a aproximadamente $929 millones de dólares estadounidenses[16]*. Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas*[17]*. El Reino Unido también sufrió el alto incremento en la práctica del phishing. En marzo del 2005, la cantidad de dinero*

---

[16] kerstein, paul: "how can we stop phishing and pharming scams?", cso, 19 de julio del 2005.

[17] kerstein, paul. "how can we stop phishing and pharming scams?", *cso*, july 19, 2005.

reportado que perdió el Reino Unido ha causa de esta práctica fue de aproximadamente £12 millones de libras esterlinas[18]".

Respuestas legislativas y judiciales

Lo bueno de estar a la vanguardia con el crecimiento tecnológico es que las leyes también se van adaptando a estos cambios y es por esto que hoy en día podemos tener respuestas judiciales y legislativas a éste tema del phishing.

A continuación se muestran varios ejemplos en los cuales se puede ver la oportuna respuesta de la ley contra los ataques de phishing en el mundo entero:

El 26 de enero de 2004, la FTC (Federal Trade Commission, "Comisión Federal de Comercio") de Estados Unidos llevó a juicio el primer caso contra un phisher sospechoso. El acusado, un adolescente de California, supuestamente creó y utilizó una página Web con un diseño que aparentaba ser la página de America Online para poder robar números de tarjetas de crédito[19]. Tanto Europa como Brasil siguieron la práctica de los Estados Unidos, rastreando y arrestando a presuntos phishers. A finales de marzo del 2005, un hombre estonio de 24 años fue arrestado utilizando una backdoor, a partir de que las víctimas visitaron su sitio Web falso, en el que incluía un keylogger que le permitía monitorear lo que los usuarios tecleaban[20]. Del mismo modo, las autoridades arrestaron al denominado phisher kingpin, Valdir Paulo de Almeida, líder de una de las más grandes redes de phishing que en dos años había robado entre $18 a $37 millones de dólares estadounidenses[21]. En junio del 2005 las autoridades del Reino Unido arrestaron a dos hombres por la práctica del phishing[22], en un caso conectado a la denominada Operation Firewall del Servicio Secreto de los Estados Unidos, que buscaba sitios Web notorios que practicaban el phishing[23].

---

[18] richardson, tim: "brits fall prey to phishing", the register, 3 de mayo del, 2005.

[19] legon, jeordan: "'phishing' scams reel in your identity", cnn, 26 de enero de 2004.

[20] leyden, john: "trojan phishing suspect hauled in", *the register*, 4 de abril del 2005.

[21] leyden, john: "brazilian cops net 'phishing kingpin'", *the register*, 21 de marzo del 2005.

[22] "uk phishers caught, packed away," *eweek*, junio 27 del 2005.

[23] nineteen individuals indicted in internet 'carding' conspiracy. 20 de noviembre del 2005.

En los Estados Unidos, el senador Patrick Leahy introdujo el Acta Anti-Phishing del 2005 el 1 de marzo del 2005. Esta ley federal de anti-phishing establecía que aquellos criminales que crearan páginas Web falsas o enviaran spam a cuentas de e-mail con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años[24].

La compañía Microsoft también se ha unido al esfuerzo de combatir el phishing. El 31 de marzo del 2005, Microsoft llevó a la Corte del Distrito de Washington 117 pleitos federales. En algunos de ellos se acusó al denominado phisher "John Doe" por utilizar varios métodos para obtener contraseñas e información confidencial. Microsoft espera desenmascarar con estos casos a varios operadores de phishing de gran envergadura. En marzo del 2005 también se consideró la asociación entre Microsoft y el gobierno de Australia para educar sobre mejoras a la ley que permitirían combatir varios crímenes cibernéticos, incluyendo el phishing[25].

¿Cómo lo denuncio?

Es muy importante tener conocimiento de la existencia de La Asociación de Internautas. En ésta las personas o mejor dicho los cibernautas pueden realizar sus denuncias ya sea por ser víctimas de phishing o por tener alguna posible víctima en la mira. Para ello deben mandar un correo electrónico a la dirección: phishing@internautas.org[26].

[24] "phishers would face 5 years under new bill," information week, 2 de marzo del 2005.

[25] microsoft partners with australian law enforcement agencies to combat cyber crime. 24 de agosto del 2005.

[26] http://seguridad.internautas.org/html/511.html.

6. COMO ESTAN ABORDANDO EL PROBLEMA LAS ENTIDADES BANCARIAS

Tomamos como base para este, algunos de los principales bancos tanto a nivel nacional como internacional. En cada uno de estos, se puede apreciar que información están brindando estas entidades a sus usuarios en línea para que se protejan a la hora de realizar cualquier tipo de transacción:

6.1. BANCOS INTERNACIONALES

6.1.1. BANK OF AMERICA

Historia

El actual Bank of America es resultado de la fusión entre Bank of America y FleetBoston Financial (empresa controladora de BankBoston).

Con esta fusión, aprobada por las autoridades en los EUA el pasado mes de Abril del 2004, se conformó el segundo banco más grande de los EUA[27] y el segundo banco más grande en el mundo[28].

Antes de esta unión, Bank of America (en ese entonces con matriz en California) y Nations Bank (con matriz en Carolina del Norte), se fusionaron, formando en ese momento el primer banco realmente nacional en los EUA, con oficinas de costa a costa y con presencia en docenas de países alrededor del mundo.

Los bancos que, mediante sus fusiones previas, conforman al actual Bank of America, han sido instituciones con personal que durante un periodo de más de 220 años han puesto sus energías para formar los cimientos del actual Bank of America. Estos bancos fueron establecidos en tiempos y en lugares diferentes. Sin embargo, todos ellos han compartido un propósito común: ayudar a sus comunidades a tener éxito y alcanzar sus sueños.

Seguridad

Protección del hurto de identidad

Bank of America ofrece una serie de herramientas que están diseñadas para ayudar a sus usuarios a proteger su nombre contra el hurto de identidad. A continuación se muestra un listado de los servicios prestados por el banco:

---

[27] valor de capitalización al cierre de la fusión en los eua en abril del 2004: $166 mil millones de dólares.

[28] valor de capitalización, y valor de capital contable al cierre de la fusión en los eua en abril del 2004: $96.5 millones de dólares.

- Acceso ilimitado en línea a las cuentas de los usuarios y a sus archivos de crédito.
- Monitoreo al crédito de sus usuarios cada día laboral con alertas cuando ocurran cambios en sus archivos de crédito.
- Total acceso a los reportes resumidos de su crédito.
- Seguro contra hurto de identidad sin costo adicional (éste seguro no está disponible para los usuarios residentes de Nueva York[29]).
- Acceso a equipos de especialistas altamente calificados que pueden ayudar a sus usuarios a entender su crédito y a luchar contra fraudes de hurto de identidad.

Prevención de fraude

1) Como Bank of America lo protege

El banco valora la confianza de sus usuarios y entiende que manejar su información financiera con cuidado es la principal responsabilidad.

a) Política de seguridad: Opera sobre detalladas políticas de seguridad que están diseñadas para proteger la seguridad y confidencialidad de la información de sus usuarios.

b) Código de ética: tienen un estricto código de ética para todas las sociedades que requieren un trato confidencial para la información de sus usuarios. Cualquier sociedad con acceso a información tiene que completar anualmente un entrenamiento de privacidad y conocimiento de la seguridad de la información.

c) Plan de seguridad computacional: el mantenimiento de la información personal y financiera de sus usuarios, de manera segura y confidencial es una de las responsabilidades más importantes. Los sistemas informáticos del banco están protegidos en los siguientes casos:

    - Antivirus: detectan y previenen virus de su sistema de red de ordenadores.
    - Paredes de fuego: bloquean accesos individuales o de redes que no están autorizadas.
    - Transmisiones de seguridad: aseguramiento del resto de la información confidencial. El banco usa una tecnología de cifrado que protege los datos en 3 formas diferentes: autenticación, encriptación e integridad de los datos.

[29] seguro subscrito por muerte a viajeros y compañía de seguridad de américa y sus afiliados. la cobertura para todas las demandas o las pérdidas, depende de calificaciones y regulaciones del estado. cobertura no disponible para los residentes de nueva york.

2) Los usuarios del banco deben de proteger su información personal

Como la información personal de las personas generalmente se encuentra en e-mails, tarjetas de crédito, identificaciones (cédula, pase), entre otras. El no proveer tanta información en los ejemplos descritos anteriormente es que se reduce el riesgo de hurto de identidad y fraude. Algunos consejos que el banco le da a sus usuarios para esto son:

- Que el cliente solo lleve con él la identificación necesaria.
- Hay que tratar las tarjetas de crédito como efectivo.
- Es necesario recupere los e-mails entrantes rápidamente. No se deben dejar estos e-mails salientes en locaciones no seguras.
- El usuario deberá hacer varias copias de toda la información financiera que lleve a diario y guardar estas copias en lugares seguros.

3) Los usuarios solo deben proporcionar información de fuentes confiables

Los usuarios deberían compartir información solamente de fuentes confiables. Si no lo hacen, pueden verificar la identidad de la fuente preguntando por su información personal, pero deberían ser muy cautelosos sobre la transacción que vayan a realizar.

4) Elimine papeles y aumente la seguridad

Estudios recientes muestran que una forma fácil de proteger la información personal es limitar la cantidad de papeles impresos que los usuarios tienen con esta información.

A continuación algunos trucos para eliminar tanto papeleo y aumentar la seguridad:

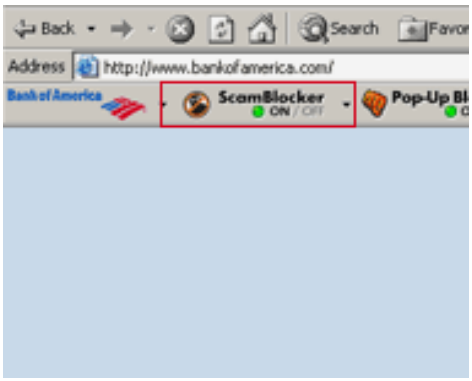
- Reducir la cantidad de e-mails que los usuarios reciben que muestran información personal.
- Botar cualquier fragmento que contenga información financiera.
- No entrar a un sitio financiero desde un link mandado al e-mail.
- No aprobar ninguna transferencia con tarjeta de crédito solicitada desde algún correo.

Barra de herramientas accionada por EarthLink® del Bank of America

Características:

Para saber si un sitio Web es seguro o potencialmente peligroso, Bank of America trabaja muy cerca a sus usuarios mientras estos

están en línea con el banco. El banco les ofrece un producto gratis que los ayuda a evitar un fraude desde cualquier lugar en Internet al que el usuario vaya. Este producto es la barra de herramientas **ScamBlocker™** mostrada por **EarthLink®**[30]. A continuación se puede apreciar esta barra de herramientas:



La seguridad de esta barra está en que alerta a los usuarios sobre algún sitio Web fraudulento que este imitando un banco legitimo.

Si un usuario visita uno de estos sitios fraudulentos el ScamBlocker™ muestra una señal en rojo de alerta. Esto quiere decir que ese sitio es potencialmente peligroso y usted no debería dar ninguna información personal. Cuando una señal amarilla es mostrada, esto quiere decir que el sitio Web es cuestionable o dudoso. Si la señal es verde quiere decir que el sitio es seguro.

Tipos de fraude en línea

E-mails y sitios Web fraudulentos

A veces los criminales tienen que enviar un e-mail que parezca que viniera de Bank of America. En este, hay un link que lleva a los usuarios a otro sitio que también luce como el banco, haciendo que los clientes llenen sus datos de cuenta personal.
Esta es una de las formas más comunes de fraude llamado "phishing and spoofing".

Spyware y virus

Ambos son programas maliciosos que son cargados en el computador sin el conocimiento del usuario. El objetivo de estos es

[30] earthlink® la proveé y opera, inc. solamente es responsable de la barra de herramientas y todas las características relacionadas con scamblocker™. cualquier reclamo deberá ser resuelto por earthlink®, el cual no está afiliado con bank of america. la herramienta no puede garantizar el encontrarse con un fraude por Internet y tampoco earthlink® y bank of america son responsables de lo que pase con su visita a cualquier sitio Web. siempre tenga cuidado al ofrecer su información personal.

capturar o destruir información para arruinar el desempeño del computador. Los virus se esparcen infectando el computador y luego se replican. Los Spyrewares se hacen ver como una aplicación legitima y se filtran en el computador, monitoreando su actividad y recolectando información.

Ventanas emergentes

Son anuncios que se muestran en ventanas separadas y cuando el usuario da clic en cualquiera de ellas es posible que pueda descargar un "spyware". Algunas veces los criminales crean estas ventanas emergentes que aparentemente vienen de instituciones financieras y preguntan por información personal financiera, pero Bank of América y la mayoría de las demás entidades financieras nunca les pedirán a sus usuarios que verifique la información financiera en estas ventanas emergentes.

Llamadas telefónicas fraudulentas

Vishing es la práctica criminal que usa ingeniería Social y voz sobre IP para acceder a información financiera privada con el propósito de recibir una recompensa. Este término es una combinación entre voz y phishing.

Cuando la víctima responde la llamada, una grabación automatizada, generada a menudo con un texto de sintetizador de discurso, es puesta para alertar al consumidor que su tarjeta de crédito ha sido víctima de una actividad fraudulenta o que su cuenta del banco ha tenido alguna actividad inusual.

El mensaje hace que el consumidor llame al siguiente número telefónico inmediatamente. El mismo número telefónico es mostrado y se da el mismo nombre de la entidad financiera que ellos pretenden representar.

Los consumidores son advertidos para que sean precavidos cuando reciban mensajes directamente a sus teléfonos para proveer información de la tarjeta de crédito y número de bancos.

Teléfonos celulares seguros

Smishing es la práctica criminal que usan técnicas de Ingeniería Social similares a las de "Phishing". Estas son las victimas que reciben mensajes de texto para que se registren en servicios en línea y luego tratan de instalarles un virus en sus dispositivos.

Algunos mensajes advierten al consumidor para ser cargados, a veces el usuario lo cancela suponiendo que van a un sitio Web; allí les extraen información como números de tarjetas de crédito y otra información privada.

Servicio de Compras seguras (ShopSafe Service®)

Comprar en línea es muy usual. Los usuarios pueden entrar al banco en línea a la opción de "ShopSafe Service®". Automáticamente se genera un número de cuenta temporal que permite completar su compra mientras le protege su privacidad.

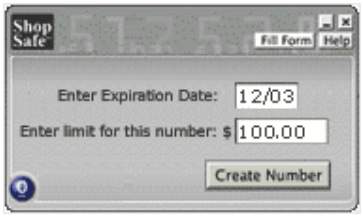
El número de cuenta son 16 dígitos que trabajan como una tarjeta de crédito regular. Cada número puede ser usado por un solo comprador en línea.

Para acceder a compra segura, los usuarios deben registrarse en la pagina del banco y escoger "ShopSafe**".**

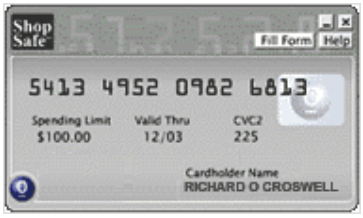
Ejemplo:

1) Comprar en línea

2) Entrar la fecha de expiración y monto



3) Crear un número de cuenta temporal que permite realizar la compra con confidencialidad



Este servicio es solo para clientes que tienen tarjeta de crédito del Bank of América y que son usuarios del servicio en línea del banco.

Regístrate

New to Online Banking? **Don't have a Credit Card?**

Enroll Now Apply Now

Detectando fraudes

Revisa tus cuentas frecuentemente

- Más del 50% de los fraudes de identidad son descubiertos por la víctima.
- Cuanto más pronto el fraude se detecta, más bajo es el impacto financiero.
- Los clientes que accedan a sus cuentas en línea detectan crímenes de identidad más rápido que aquellos que confían en e-mails.
- Los clientes que tienen alarmas en los e-mails para que les envíen notificaciones de actividades importantes en sus cuentas, pueden ayudar a identificar fraudes más rápidamente.

Practicas en línea de políticas de aislamiento

Navegando por nuestro sitio Web

El usuario puede navegar por el sitio Web del banco anónimamente sin dar información personal que lo identifique, como nombre ó e-mail. Si navega de esta manera, el banco no podrá enviarle links para que realice actividades en línea con alguna de las cuentas que tiene.

Navegar luego de haber sido identificado implica inhabilitar las cookies del sistema y archivos similares o borrando las cookies y archivos similares que usted acepto del banco. Para hacer esto, necesitará seguir las instrucciones de navegación para deshabilitar o borrar las cookies.

Cookies y archivos similares

En todos los casos las cookies y archivos similares que el banco descarga en el computador no contienen información personal. Esta descarga se realiza con el propósito de seguridad, facilitar la navegación y personalizar la experiencia de los usuarios mientras visitan el sitio Web. Estas cookies no revelan la identidad de los usuarios ni su número de cuenta. Si el usuario no acepta estas cookies o archivos similares experimentara algunos inconvenientes en el uso de productos en línea. Por ejemplo para banca en línea, el banco no esta habilitado para reconocer los computadores y el usuario necesitará responder una serie de preguntas cada vez que se registre en la página.

Bank of América usa las cookies en dos formas:

1) Cookies de navegadores de Web

Estas pueden contener una variedad de información como un contador que mida cada cuanto entra usted a este sitio Web. Las cookies permiten recolectar información técnica y de navegación como tipo de navegador, tiempo que tarda en el sitio y páginas visitadas.

2) Banca en línea
Bank of América usa las cookies durante la sesión en línea. Por ejemplo, para el mejoramiento continuo del diseño y funcionalidad para prestarle un mejor servicio.

3) Archivos similares
Algunos sitios Web usan tecnologías similares a las cookies para el almacenamiento de información.[31]

6.1.2. HSBC

Historia

HSBC es un banco global que cuenta con una red internacional de 10,000 oficinas distribuidas en más de 80 países de Asia, Europa, Norte América, Latinoamérica, el Medio Oriente y África. HSBC emplea a más de 260,000 personas y atiende a más de 125 millones de clientes.

Desde el 2007, América es el continente en el cual HSBC tiene el mayor número de empleados. Con más de 68,000 colaboradores en 16 países, HSBC tiene una cobertura a lo largo de todo el continente, desde Canadá hasta Argentina.

El desarrollo de esta red en América es producto de un agresivo plan de expansión regional desde mediados de los 90, complementada con recientes adquisiciones y apertura de nuevos negocios.

En 1997, HSBC adquiere el Banco Roberts en Argentina con negocios de banca, seguros, EPS y fondos de pensiones y en el mismo año adquiere el Banco Bamerindus en Brasil, país en el que HSBC cuenta hoy con más de 28,000 empleados.

Consolidando su presencia en los mercados más importantes del continente, en el 2000 adquiere Bital, el cuarto grupo financiero de México.

---

[31] https://www.bankofamerica.com/index.jsp.

En el 2003 consolida su posición de liderazgo en Financiamiento de Consumo con la adquisición de Household International, la segunda financiera de consumo de Norte América y la compra de Losango en Brasil.

La expansión del grupo durante el 2006 incluyó la compra del BNL en Argentina, las operaciones de Lloyds en Paraguay, el inicio de operaciones en el Perú y el anuncio en Julio de la adquisición de Banitsmo, el principal banco de Centro América con operaciones en Panamá, Colombia, Costa Rica, Nicaragua, Honduras y El Salvador.

Seguridad

Para HSBC es de suma importancia el manejo y confidencialidad de la información que suministran sus usuarios a través de la página Web. Por eso, en lo relacionado con este tema, HSBC manifestarte que:

- Toda la información que HSBC pide y que efectivamente nos suministran los usuarios es considerada por HSBC como información personal y confidencial. Por lo tanto HSBC le aplica a la misma, la protección y seguridad necesaria.
- La información que HSBC obtiene de sus usuarios a través de la página Web no será divulgada a ningún tercero, excepto que medie orden de autoridad para el efecto o que por ley HSBC deba proceder a dicha divulgación total o parcialmente. En cualquier otro caso, HSBC pide la autorización de sus usuarios antes de divulgar la información que estos han suministrado y el banco no procederá a divulgarla sin contar con dicha autorización.
- La información que los usuarios suministran en la página Web no será vendida, arrendada ni comercializada por HSBC a ningún tercero, probablemente, la misma será empleada dentro del Grupo HSBC, es decir, con nuestras filiales o subsidiarias, o nuestra casa matriz, sus filiales o subsidiarias. En cualquier caso, esa información sólo será usada para la promoción de los servicios de HSBC y productos y con el fin de mantener a sus usuarios actualizados sobre las actividades del banco.
- Desde el momento que el usuario ingresa su información en la página de HSBC, la misma está siendo protegida por sistemas de encripción desarrollados al interior del banco.
- El usuario podrá cambiar, modificar o actualizar, total o parcialmente y en cualquier tiempo, la información que le ha suministrado al banco.
- Los correos electrónicos que se envían por la red no gozan necesariamente de absoluta protección, por ende la información que el usuario envía por esa vía podría ser leída por terceros. Por

lo anterior, el contenido de los correos electrónicos que envían los usuarios no es completamente seguro y ellos asumen ese riesgo al contactar al banco por dicha vía.

- Para ofrecer una experiencia de exploración más personalizada, la página Web de HSBC guardará un pequeño archivo de texto (llamado "cookie") en el disco duro del computador de los usuarios, el cual se elimina tan pronto como ellos abandonen la página Web. Este archivo sólo será usado para recoger información sobre las preferencias de los usuarios para facilitarles posteriores consultas. En todo caso, ellos podrán rechazar la instalación de dicho archivo desde la configuración de su navegador.

A nivel mundial, personas inescrupulosas están enviando correos electrónicos para ponerse en contacto con clientes, utilizando mensajes que imitan, casi a la perfección, el formato, lenguaje y la imagen de las entidades bancarias // financieras, y que siempre incluyen una petición final en la cual se solicita la conexión a una dirección Web para que el cliente "confirme" determinados datos personales alegando distintos motivos: problemas técnicos, cambio de política de seguridad, posible fraude, etc.

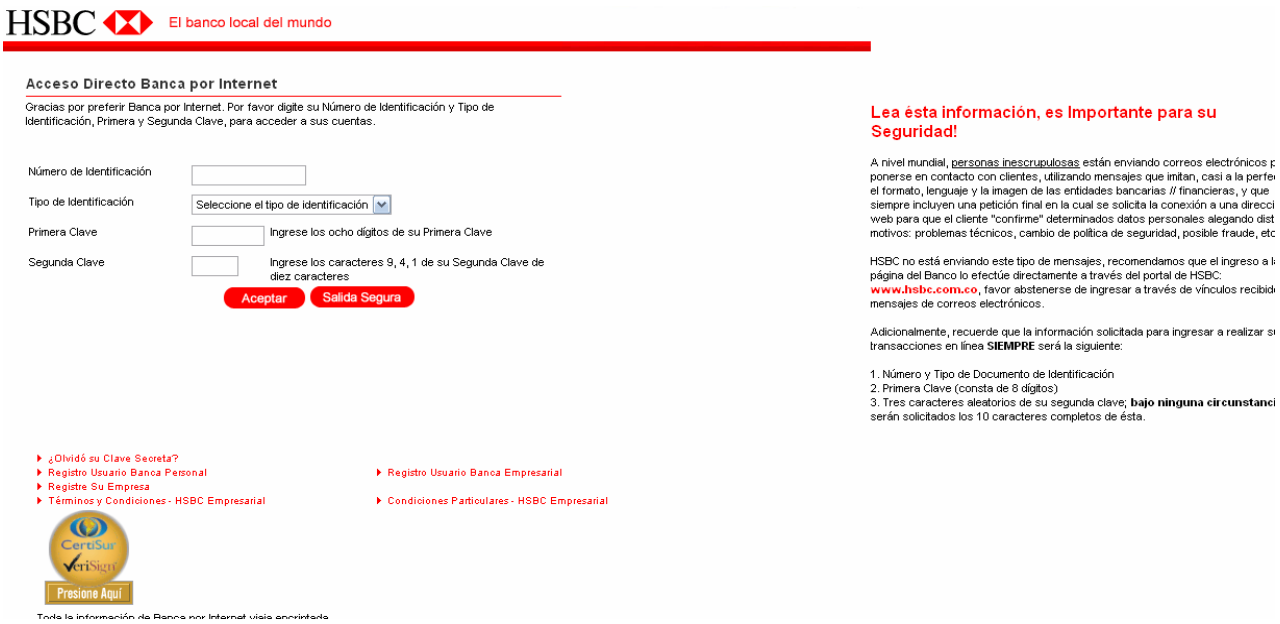
HSBC no está enviando este tipo de mensajes, por lo que recomiendan que el ingreso a la página del Banco sea efectuado directamente a través del portal de HSBC: ww.hsbc.com, además le piden el favor a los usuraos que se abstengan de ingresar a través de vínculos recibidos en mensajes de correos electrónicos.

Adicionalmente, los usuarios deben recordar que la información solicitada para ingresar a realizar sus transacciones en línea SIEMPRE será la siguiente:

1. Número y Tipo de Documento de Identificación.

2. Primera Clave (consta de 8 dígitos).

3. Tres caracteres aleatorios de su segunda clave; bajo ninguna circunstancia le serán solicitados los 10 caracteres completos de ésta.



5 Reglas de Oro

1) Actualizaciones y parches

Año tras año vulnerabilidades en los programas de computador son descubiertas. Estas debilidades son corregidas con parches y actualizaciones.

2) Anti virus

El usuario deberá tener su software con las últimas actualizaciones de antivirus. Hay varios programas efectivos, los mas comunes son: McAfee, Symantec (Norton) y Sophos.

3) Paredes de fuego personales

Estos son otros pequeños programas que ayudan a proteger su computador. Evitan el tráfico no autorizado para su PC.

4) Consejos para contraseñas

Una contraseña es la llave para acceder a información de la cuenta en línea. El usuario deberá evitar usar la misma contraseña en diferentes sitios.

Cuando el usuario escoja una contraseña debe considerar lo siguiente:

- Evite usar la misma contraseña para servicios diferentes.

- No usar contraseñas que sean relacionadas a su vida personal. Nombre de sus hijos, mascotas, fecha de nacimiento o números telefónicos.
- No escribir ni guarde sus password.
- Nunca divulgar su información en línea, excepto que use el sitio Web seguro de su banco, el cual nunca viene adjunto en un link vía e-mail.

5) Antispyware

Es el término que se usa para describir programas que corren en los computadores con el propósito de monitorear y guardar el camino en el que el usuario navega en la Web y los sitos de Internet que visita. Por ejemplo, el spyware puede combinar información sobre el comportamiento en línea de sus usuarios con el de otros usuarios para generar datos de búsqueda. Esta información puede ser vendida y comprada por compañías interesadas en promover la manera en que los sitios Web son diseñados y como es usado el Internet.

Aseguramiento de las actividades bancarias

Seguridad en línea- Pasos que tomamos

Como banco HSBC piensa en la seguridad. El crecimiento del Internet ha ofrecido una gran flexibilidad, pero también un nuevo riesgo. HSBC usa una tecnología de seguridad estándar para la industria y prácticas enfocadas en tres aéreas: privacidad, tecnología e identificación para guardar la seguridad de las cuentas de sus usuarios de cualquier acceso no autorizado.

Seguridad en línea- Pasos que puede tomar

Hay más que los usuarios puedan hacer para protegerse en línea. Algunas cosas son simples y otras requieren de un poco más de tiempo o ayuda de alguien más.

Nuestros pasos

Privacidad

HSBC usa la industria de encriptación estándar dentro de sus servicios bancarios en Internet

Sesiones de seguridad

Cuando el usuario inicia una sesión en línea en un banco, éste dice que es una sesión segura. El usuario sabe que es así si la

dirección URL empieza por **https:**// o por que aparece un símbolo de seguridad (candado) en la parte inferior derecha de su navegador.

Encripción

Esta tecnología es usada dentro de las sesiones bancarias en Internet para encriptar información personal en caso de dejar solo el computador y alguien mas pueda leer esta información. Dependiendo de la configuración del navegador, las ventanas emergentes aparecerán para notificar el ingreso a una página segura.

HSBC usa 128 bits SSL (Secure Sockets Layer) de encripción, lo cual es aceptado en el nivel estándar de la industria.

Tiempo suficiente de sesión

Si el usuario olvida cerrar la sesión de banco en línea o el computador esta inactivo por un periodo largo, el sistema se cerrará automáticamente. Las páginas vistas durante una sesión segura no son recordadas en los archivos temporales los computadores.

Tecnología

HSBC usa muchas capas de seguridad, como:

- El sistema operativo esta actualizado con las últimas versiones de parches.
- El anti virus se mantiene actualizando.
- HSBC usa paredes de fuego para prevenir intrusos.

Identificando la privacidad

- HSBC usa claves de acceso para asegurarse que esta tratando con sus clientes.
- Cerrar sesión automáticamente.

Sus usuarios deben mantener segura su sesión bancaria en Internet

Tips

1. Memorizando la clave de acceso.

2. No usando links de otras partes para acceder al sitio Web de HSBC.

3. Evitando usar computadores compartidos para sus actividades bancarias.

El usuario debe mantener su e-mail seguro

Generalmente los e-mails que son recibidos o enviados a través de direcciones regulares no son seguros ni cifrados. Por lo tanto cualquier información personal que el usuario incluya en un e-mail esta en riesgo de ser interceptada por individuos no autorizados. El usuario no deberá enviar sus contraseñas e identificaciones bancarias por este medio.

Phishing

El phishing implica el envió de e-mails a diferentes direcciones de Internet. La característica de estos e-mails es que parecieran que vinieran de organizaciones legítimas como bancos pagos en línea, etc. El e-mail le solicita al usuario verificar su información personal y financiera incluyendo fecha de nacimiento, contraseñas, número de tarjetas de crédito, etc. El objetivo es inducir a los usuarios a que sean clientes de la organización legítima que esta siendo imitada.

El e-mail contiene links que lo llevan a sitios que son "idénticamente" iguales al que el usuario cree estar visitando. Dando clic en este link también se puede estar bajando software maliciosos como spyware en el computador del usuario engañado.

Mulas

Cuando la información ha sido obtenida mediante un ataque de phishing, hay personas esperando por esta para proceder a realizar robos con cuentas que no los comprometan. Sin embargo, reclutan a individuos para que actúen como mediadores ofreciéndoles oportunidades de trabajo o ganar dinero sin realizar el mayor esfuerzo. A estos individuos se les conoce como mulas.

Las cuentas bancarias de las mulas serán utilizadas para aceptar transferencias del dinero de las cuentas comprometidas. A las mulas se les pedirá retirar el dinero de sus cuentas en efectivo y remitir este dinero sacando su comisión a los que realizaron el fraude mediante una agencia internacional de transferencia de dinero. Por lo tanto los que realizan este fraude pueden

permanecer en el anonimato, pero sí hay forma de que las autoridades rastreen a las mulas.

Los usuarios deberán tener mucho cuidado sobre las ofertas de trabajo que implican la aceptación y el traslado de fondos a una cuenta bancaria para que estos reciban alguna comisión.

Recursos

Para mayor información visite los sitios que se listan a continuación:

Anti virus

Los más populares son:

- McAfee
- Symantec (Norton)
- Sophos

Paredes de fuego

Ejemplo de las más comunes comercialmente:

- Zone Labs
- Symantec (Norton)
- McAfee
- Computer Associates

Anti gusanos

Los más usados:

- Symantec (Norton)
- McAfee
- Sophos

Anti spyware

Programas que detectan y le ofrecen la decisión de escoger cual spyware desea eliminar:

- Lavasoft's Ad-aware
- PepiMK's Spybot Search & Destroy [32]

[32] http://www.banistmo.com.co/

6.1.3. JPMORGAN CHASE

Historia

Es una empresa financiera creada el año 2000 a partir de la fusión del Chase Manhattan Corporation y la J.P. Morgan & Co. (Banca Morgan). Es una de las empresas de servicios financieros más antiguas del mundo. La empresa, con oficina central en Nueva York, es líder en inversiones bancarias, servicios financieros, gestión de activos financieros e inversiones privadas. Con activos financieros de 1,3 billones de dólares, JPMorgan Chase es actualmente la tercera institución bancaria de Estados Unidos[33], detrás del Bank of América y el Citigroup.

La unidad de fondos de inversión libre (hedge fund) del banco es la más grande de los Estados Unidos con inversiones por 34 mil millones de dólares en 2007[34].

En 2004, la empresa volvió a fusionarse con el Bank One de Chicago, incorporando al CEO de éste último, Jamie Dimon como presidente y COO de la empresa fusionada, al mismo tiempo que se resolvió que sería el sucesor de quien era CEO del grupo en ese momento, William B. Harrison, Jr. En enero de 2006, Dimon fue finalmente nombrado CEO y en diciembre también presidente del JP Morgan Chase.

JPMorgan Chase opera como marca del holding. *Chase* se usa como marca de las tarjetas de crédito y las actividades bancarias minoristas en los Estados Unidos.

Seguridad

Como te protegemos

Para la seguridad de los usuarios deben ser cuidadosos con su información al acceder a su cuenta en línea. Deben entrar desde la página del banco directamente creando un usuario y contraseña que solo usted sepa.

---

[33] http://www.ffiec.gov/nicpubweb/nicweb/top50form.aspx

[34] http://www.marketwatch.com/news/story/jp-morgan-tops-ranking-us/story.aspx?guid=%7b99bbeed2-81cb-42ad-bb19-8cb38b45d97d%7d

JPMorgan Chase usa la tecnología de SSL (Secure Socket Layer) para encriptar su información personal como contraseñas, usuarios, etc.

Como JPMorgan Chase protege a sus usuarios

El banco usa una gran variedad de tecnologías y técnicas para asegurarse que sus productos y servicios son seguros.
A continuación algunos pasos que los usuarios pueden seguir:

- El usuario deberá hacer lo que pueda para prevenir que personas no autorizadas usen su computador.
- Cerrar su sesión o bloquear su estación de trabajo cuando dejan su computador.
- Cambiar sus contraseñas cada vez que puedan. Asegurándose de escoger contraseñas que sean difíciles de adivinar.
- No dar sus contraseñas a nadie y no grabarlas en lugares fáciles de encontrar.
- Al notar alguna actividad sospechosa en su cuenta, reportarla de inmediato.
- Instalar anti virus, anti syware y demás software para seguridad en Internet.
- Estar alerta a e-mails que provengan de personas que el usuario no conoce.
- Asegurarse de que el navegador encripte la información personal.

Phishing
Forma de actividad criminal que emplea técnicas de Ingeniería Social para adquirir información sensitiva como contraseñas y detalles de las tarjetas de crédito. Aquellos que lo realizan aparentan ser personas confiables o de negocios electrónicos oficiales.

- **Que protección deben tener los usuarios para responder a un ataque de phishing?**

Cada situación es diferente. Ellos tienen que tomar la mejor decisión basado en la naturaleza del compromiso y que datos va a compartir.

- **El usuario deberá dar su usuario o contraseña en e-mails?**

Nunca debería dar esta información a alguien.

- **Como lucen los e-mails fraudulentos?**

Toman formas diferentes, pero la mayoría son muy similares a los sitios reales.

- **Qué debe hacer el usuario si tiene un e-mail sospechoso sin el logo del banco?**

No lo reenvié, ni de clic sobre este ni entre alguna información. Si este dice que viene del banco JPMorgan Chase, reenvíelo a la dirección abuse@chase.com.

- **Cuando un e-mail puede ser falso si dice que viene de Chase, enviado a la dirección del usuario y con su nombre?**

Es el resultado de un nuevo tipo de fraude llamado "spear phishing". Los grupos criminales recolectan datos de múltiples recursos combinados para crear e-mails más convincentes y así usted comparta su información.

No son las prácticas de JPMorgan Chase:

- Enviar e-mails que requieran que entre información personal directamente al e-mail.
- Enviar e-mails que dicen que si no adjunta su información personal le cerraremos la cuenta.
- Enviar e-mails preguntando que lo reenvíen con información personal.
- Compartir su nombre con otras personas. [35]

6.1.4. THE ROYAL BANK OF SCOTLAND GROUP

Historia

En un negocio donde la discreción es fundamental, nuestro propósito ha consistido no tanto en ser conocidos por muchos, sino en despertar confianza en una minoría con criterio propio. Desde empresarios hasta celebridades o aristócratas, la clientela de Coutts no podría ser más diversa. Fundado en Londres en 1692, Coutts ha atraído como clientes a muchos personajes de fama mundial, entre los que cabría citar, por ejemplo, a Charles Dickens, Frederic Chopin o Lord Alfred Tennyson.

Coutts International forma parte del Grupo The Royal Bank of Scotland, constituido en 1727 y actualmente una de las entidades bancarias más grandes del mundo. Nos enorgullece pertenecer a esta distinguida institución financiera. La continuidad y la tradición tienen una gran importancia en nuestra historia. Nuestros valor es más apreciados han sido siempre, por un lado, el respeto a la privacidad y, por otro, la conservación y el crecimiento del patrimonio de nuestros clientes. Estos principios forman los cimientos de toda

[35]http://www.jpmorganchase.com/cm/satellite?c=page&cid=1159304834085&pagename=jpmc/page/new_jpmc_homepage

nuestra filosofía de negocio y de los servicios que prestamos y seguiremos prestando en el futuro a nuestros clientes.

Durante muchos años, esta combinación de tradición y servicio personal ha permitido a Coutts International mantenerse a la vanguardia en la gestión de patrimonios para una clientela altamente sofisticada[36].

Seguridad

Seguridad bancaria en línea

Para los usuarios mantenerse seguros mientras navegan, deben seguir los siguientes pasos:

El usuario deberá proteger su computador

Para esto necesitara software como, antivirus, pared de fuego y asegurarse que su sistema operativo tenga las siguientes actualizaciones:

1) Instalar anti virus

- El anti virus protege el computador de dos maneras diferentes. La primera es detectando y removiendo virus y spyware de cualquier computador. La segunda es previniendo la infección del computador con virus y spyware.

2) Mantener paredes de fuego

- Es una aplicación que ayuda a evitar el acceso de personas no autorizadas a su computador en línea.

3) Asegurarse de mantener los software de su computador actualizados 3537656

Mantenga su identidad segura

1) Detalles de seguridad

THE ROYAL BANK nunca le pide a sus usuarios que den su contraseña completa sino que le pide parte de ella al acceder al servicio bancario en Internet.

[36] https://www.bank-von-ernst.ch/files/secure/imagebrochure_s.pdf

El número de seguridad y contraseña son claves para las cuentas de los usuarios en línea. Ellos deberán mantenerlas en lugares seguros, nunca deberán compartir con alguien más y cambiar la contraseña con regularidad.

2) E-mails fraudulentos o "phishing"

Phishing es una técnica muy común que hace que la gente revele su información personal como claves, números de seguridad, entre otras.

A continuación esta cómo funcionan los ataques de phishing: Los criminales envían e-mails que lucen como lugares de buena reputación. Este e-mail falso le pregunta por detalles de seguridad, contraseñas, usuarios, etc. Ellos roban sus datos y cometen fraude.

Si sospecha de ser víctima de un ataque de phishing llámenos al teléfono **0845 600 8212** o escribanos digitalbanking@rbs.co.uk.

Seguridad en línea

1) El usuario deberá chequear la seguridad en sitios Web comerciales y bancarios

- El usuario siempre digitará el mismo la dirección URL www.rbs.co.uk directamente en su navegador. Esto reduce los ataques de phishing.
- El usuario deberá chequear el "https" y el candado de seguridad. Las paginas son seguras si la dirección URL tiene en el inicio https y muestra un candado en la parte inferior del navegador.
- El usuario deberá dar doble clic en el candado que aparece en la parte inferior del navegador para ver la información sobre la seguridad y como puede confirmar si el sitio es o no genuino. Si el candado no tiene fecha valida o presenta cualquier otra anomalía, no entre sus detalles de seguridad y comuníquese con nosotros.

2) Siempre deberá cerrar la sesión en sitios seguros. Nunca deje su computador sin cerrar la sesión que tiene iniciada.
3) El usuario deberá ser muy cuidados cuando use los computadores en lugares públicos.[37]

6.1.5. SANTANDER

[37] http://www.rbs.co.uk/

Historia

La historia del Santander comienza el 15 de mayo de 1857, cuando la Reina Isabel II firma el Real Decreto que autoriza la constitución del Banco de Santander. Desde sus orígenes fue un banco abierto al exterior, inicialmente ligado al comercio entre el puerto de Santander, en el norte de España e Iberoamérica.

Entre los años 1900 y 1919 el Banco Santander dobló su balance, amplió su capital hasta los diez millones de pesetas, aumentó sus ingresos, se acercó a la cifra de medio millón de pesetas de beneficios en el ejercicio de 1917 y su rentabilidad se colocó por encima de la media de las sociedades de crédito españolas. Además, durante estos años, se fundan los tres grandes bancos españoles que con el tiempo se integrarán en el Santander: el Banco Hispanoamericano (1900), el Español de Crédito (1902) y el Central (1919).

En enero de 1999 Banco Santander y BCH protagonizan la primera gran fusión bancaria en la Europa del euro. Nace así la mayor entidad financiera de España y líder en Iberoamérica. Posteriormente el Banco compra en Portugal el Grupo financiero Totta y Açores y Crédito Predial Portugués.

A partir del año 2000 se incorporan al Grupo, Banespa en Brasil, Grupo Serfín en México y Banco Santiago en Chile. Con ello se afianza la posición del Grupo como primera franquicia financiera en Latinoamérica.

En abril de 2004 se realizó el traslado de los servicios centrales en Madrid a la nueva Sede Corporativa, la Ciudad Santander, en la que hoy trabajan 6.800 profesionales.

En 2005 Santander llega a un acuerdo para la toma de participación del 19,8% en Sovereign Bancorp, banco número 18 de los Estados Unidos.

En 2006 el Santander obtiene un beneficio récord de 7.596 millones de euros, el mayor de cualquier empresa española e impulsa una fuerte inversión en la banca a clientes y calidad de servicios. “Queremos ser tu banco” en España y otras acciones emprendedoras en Portugal, Abbey y América, son ejemplos de este esfuerzo.

En 2007 Santander celebra su 150 aniversario siendo el duodécimo banco del mundo por capitalización bursátil, el séptimo por beneficios y la entidad con la mayor red de distribución minorista del mundo occidental: 10.852 oficinas.

Seguridad

Recientemente, han sido detectados e-mails fraudulentos enviados a clientes de diferentes Entidades Financieras, solicitando sus datos o claves de acceso a Banca Electrónica. Para evitar ser víctima de un fraude, los usuarios nunca deberán atender a solicitudes de claves que le lleguen a través de correo electrónico, y además:

- Su usuario, contraseña, pin de tarjeta, firma, etc. son datos de carácter personal y estrictamente confidenciales, solo deben ser usados para el acceso a los servicios propios de Santander.

- Como usuario deberá desconfiar de cualquier toma de datos personales realizada a través de Internet, en nombre de Santander, y fuera de su sitio Web seguro. Ante cualquier duda de la veracidad de los datos pedidos o autenticidad de las páginas visitadas, le ruegan a sus usuarios que se contacten de manera inmediata con Santander por los canales establecidos. Ninguna Empresa del Grupo Santander le requerirá información que ya deba estar en su poder.

- No deberá dar nunca información personal o financiera en respuesta a un e-mail.

- No utilizar los enlaces incorporados en e-mails o páginas Web de terceros.

Para ampliar información referente a cómo se debe actuar y que medidas deben tomar los usuarios contra el robo de identidad y el fraude on-line deberán consultar www.nomasfraude.es.

El servidor de Santander posee un certificado emitido por una autoridad certificadora internacional (Verisign Inc.). Este certificado garantiza que realmente se ha conectado con Banco Santander y que los datos transmitidos son cifrados. El usuario podrá verificarlo pinchando sobre el candado que aparece en la parte inferior derecha del navegador.

Conexiones Seguras SSL: Santander dispone de un sistema de seguridad que garantiza la integridad y la confidencialidad de los datos que se intercambien entre el cliente y Banco Santander. Toda la información sensible es transmitida por la red encriptada mediante protocolo SSL y claves de 128 bits. Este sistema impide que terceras personas puedan ver o modificar dichos datos.

Santander le ayuda a conocer si su navegador cumple con estos requisitos de seguridad:

- Si utiliza Netscape Navigator 4 ó superior o Internet Explorer 5.5 ó superior ya dispone de intensidad de cifrado de 128 bits.
- Si utiliza Internet Explorer inferior a 5.5 verifique la Intensidad de Cifrado de su navegador:
    - El usuario deberá seleccionar "Ayuda"/"Help" en el menú superior.
    - Seleccionar "Acerca de Internet Explorer"/"About Internet Explorer".
    - Internet Explorer muestra un cuadro donde se puede comprobar la Intensidad de Cifrado que esta instalada. En el caso en que ésta sea inferior a 128 bits pulse sobre "infor.actualización" lo que le llevará a las páginas de Microsoft donde podrá actualizar a 128 bits la Intensidad de Cifrado de su navegador.
    - Una vez realizada dicha actualización podrá acceder a la banca on-line de Santander.

Autoridad Certificación: El servidor de Santander pose un certificado emitido por una autoridad certificadora internacional (Verisign Inc.). Este certificado garantiza que realmente se ha conectado con Banco Santander y que los datos transmitidos son cifrados. El usuario podrá verificarlo pinchando sobre el candado que aparece en la parte inferior derecha de su navegador.

Privacidad: se le recuerda al cliente que su usuario, contraseña, pin de tarjeta, firma, etc. son datos de carácter personal y estrictamente confidenciales, solo deben ser usados para el acceso a los servicios propios de Santander. La cesión de los datos confidenciales a terceras personas es responsabilidad del propietario de los mismos.

Santander ruega a sus usuarios que desconfíen de cualquier toma de datos personales realizada a través de Internet, en nombre de Santander, y fuera de su sitio Web seguro. Ante cualquier duda de la veracidad de los datos pedidos o autenticidad de las páginas visitadas, Santander pide a sus clientes que se contacten de manera inmediata con el banco por los canales establecidos en la página principal.

Al usuario acceder a las páginas del Banco se ejecutan módulos de seguridad en programas Java, lo que hace al servidor aun más seguro, y por ello es imprescindible que el usuario tenga todas las opciones de Java activadas en su navegador.

Por último, Santander ofrece una serie de consejos para la protección de su ordenador personal y de la información que contiene:

- El usuario deberá actualizar el ordenador personal con las últimas actualizaciones de seguridad recomendadas por el fabricante.
- El usuario deberá proteger el ordenador personal con un software antivirus convenientemente actualizado, que evite infecciones de virus.
- El usuario deberá mantener una copia de seguridad de la información contenida en el ordenador personal. [38]

6.2. BANCOS NACIONALES

6.2.1. BANCO DE BOGOTÁ

Historia

El Banco de Bogotá inició sus labores el 15 de noviembre de 1870 como primera institución financiera creada en el país, con un capital de $500.000 y con la facultad de emitir billetes. Su primer Director - Gerente fue el señor Salomón Koppel.

2000 con La Corporación de Ahorro y Vivienda AHORRAMAS, cambiando su denominación por AV VILLAS.

En junio de 2001 el Federal Reserve aprobó la solicitud de conversión del Banco de Bogotá International Corporation en Agencia, establecida en el Estado de La Florida de los Estados Unidos. Esta conversión se llevó a cabo en el segundo semestre de 2001. El Banco de Bogotá Colombia poseía indirectamente a través de su filial Banbogotá INC el 100% de participación de Banco de Bogotá International Corporation.

En el 2003 el Banco y sus filiales Fiducomercio y fiduciaria Bogotá compraron el 11.67% de la Sociedad Administradora de Fondos de Pensiones y Cesantías Porvenir S.A. al grupo Provida Internacional S.A.

En la actualidad, Banco de Bogotá cubre la totalidad del territorio nacional, gracias a sus 275 oficinas, 5 centros de servicios

[38] www.bancosantander.com

corporativos, 1 centro de atención bancaria, 24 cajas remotas, 14 Centros de Pago y 3 Kioscos, ubicados en 120 municipios del país. Adicionalmente, dispone de un completo portafolio de productos y servicios electrónicos y de un dinámico portal www.bancodebogota.com, que le permite ofrecer sus servicios las 24 horas del día, todos los días del año, desde cualquier lugar del mundo.

Además, Banco de Bogotá desarrolla operaciones internacionales a través de los convenios que tiene con los bancos corresponsales en todo el mundo y a sus filiales y agencias en el exterior – Panamá, Nassau, Miami y Nueva York.

Seguridad

Cuidado con el Phishing

El banco está comprometido con sus usuarios. Por eso traba para brindarle privacidad y confidencialidad a su información. Por la seguridad de estos, el banco presenta información y recomendaciones importantes sobre la modalidad de fraude en Internet conocida como phishing.

Qué es Phishing?

El Phishing (pesca de información) es una modalidad de fraude de Internet, que utiliza mensajes de correo electrónico "engañosos" y sitios Web fraudulentos, diseñados para confundir a los destinatarios para que divulguen información financiera personal, como números de Tarjeta de Crédito, o Débito, contraseñas, nombre de usuario u otros datos personales como cédula o Nit.

Cómo detectarlo?

Los ciberdelincuentes envían un correo electrónico a nombre de entidades financieras de confianza, incluyendo situaciones de urgencia para que las personas reaccionen de manera inmediata y respondan con la información que ellos desean. Generalmente, incluyen un vínculo falso que parece llevarlo al sitio Web legítimo que están suplantando, pero en realidad lleva a un sitio falso o incluso a una ventana emergente con el mismo aspecto del sitio Web oficial de la entidad financiera.

En el Banco de Bogotá asumen el compromiso de proteger la privacidad y seguridad de sus usuarios, por lo que les dan las siguientes recomendaciones:

- Mantener actualizado el equipo con los últimos parches de seguridad de sistema operativo.
- Instalar sistemas de antivirus y firewalls personales en sus equipos.
- No diligenciar formularios que vengan dentro de los correos electrónicos
- Nunca responder a solicitudes de información personal a través de correo electrónico.
- Para visitar sitios Web, introducir la dirección URL en la barra de direcciones.
- Consultar frecuentemente los saldos bancarios y de sus tarjetas de crédito.
- Cambiar sus claves frecuentemente.
- Comunicar los posibles delitos relacionados con su información personal a las autoridades competentes

Recuerde:

- Ningún funcionario del Banco esta autorizado para solicitar información de autenticación (nombre de usuarios y contraseñas).
- NO es política del Banco enviar correos electrónicos solicitando actualización de información confidencial (número de tarjeta, documento de identidad. claves).
- Si el usuario recibe un correo electrónico donde se solicite información confidencial como claves, número de tarjetas o usuario, se le pide el favor de informar inmediatamente al Banco de Bogotá a servicioalcliente@bancodebogota.com.co, anexando el correo recibido.

www.bancodebogota cuenta con la certificación de Verising para ofrecerles a sus usuarios transacciones seguras.[39]

6.2.2. BANCO DE OCCIDENTE

Historia

El Banco de Occidente inició operaciones como sociedad anónima comercial de naturaleza bancaria, debidamente constituida, el 3 de mayo de 1965, bajo la administración del Doctor Alfonso Díaz.

Su orientación y su rango conservaron inicialmente el matiz regional durante los primeros años, período durante el cual el desarrollo del sector bancario fue realmente lento.

[39]www.bancodebogota.com

En 1973 El Banco de Occidente inició una nueva etapa bajo la orientación del grupo económico Sarmiento Angulo, el cual lo fortaleció con recursos de capital y su reconocida experiencia, transformando profundamente la institución y ampliando sus horizontes, hasta convertirla en una entidad de proyección nacional e internacional.

Al llegar 1980 el Banco ha desarrollado ya considerablemente su red de oficinas y su envergadura financiera, lo que lo lleva a formar Direcciones Regionales. En diciembre de ese año el Banco cuenta con 80 oficinas, activos por 16.000 millones de pesos y un patrimonio de 1.875 millones de pesos.

En el año 2000 se desarrolló el proyecto MCKINSEY, con el cual sé rediseñó la estructura organizacional del Banco buscando mayor eficiencia y productividad administrativa en todas las áreas staff del Banco.
El Banco de Occidente considera haber cumplido y estar cumpliendo un compromiso de desarrollo en el país, respondiendo a la confianza de la comunidad, de sus clientes y de sus accionistas.

Seguridad

Compromiso de seguridad del Banco de Occidente

En el Banco de Occidente asumen el compromiso de proteger a sus clientes en privacidad y seguridad. Nunca les solicita información confidencial por ningún medio como número de documento de Identidad, Usuario o Login en Internet, Contraseña, Claves. Por su seguridad, el banco les aconseja no compartir esta información personal con nadie.

Al Ingresar a la página...

- Cuando el usuario ingresa a la zona transaccional, solamente tendrá que digitar su usuario y contraseña. Nunca el Banco le solicita estos datos secretos a través de correos electrónicos, ni por ningún otro medio.
- Ingresar al Banco por Internet siempre en forma directa digitando en el explorador de Internet www.bancodeoccidente.com.co. Nunca hacer clic en correos electrónicos que contengan links hacia la página.

Con su usuario y contraseña...

- Realizar transacciones por Internet desde el computador personal de la casa u oficina, en algunos sitios públicos pueden instalar programas para rastrear sus operaciones.
- Nunca utilizar a terceras personas para realizar las operaciones, hágalas siempre personalmente.
- Memorizar su usuario y contraseña y mantenerlas en absoluta reserva.
- Por seguridad nunca suministrar información personal (usuario, contraseña, número de cuenta o documento de identidad) a personas que lo soliciten bajo el argumento de participar en concursos, premio o cualquier otro tipo de ofertas.
- No construir la contraseña con fechas de nacimiento, número de documento de identidad o números de dirección y/o teléfono.
- El banco de occidente esta certificado VeriSign .[40]

6.2.3. DAVIVIENDA

Historia

En sus inicios, se centró en la actividad aseguradora, específicamente de personas, a través de la Compañía de Seguros Bolívar S.A., fundada el 5 de diciembre de 1939, con la que incursionó en un mercado conformado por diversas aseguradoras internacionales, y La Compañía Colombiana de Seguros, que por esos días era la única del capital colombiano.

La confianza que mereció en el mercado por la prestancia de sus accionistas y el acertado manejo del negocio, fundamentado en sólidos principios éticos, comerciales y sociales, fue factor determinante para su dinámico crecimiento, y la consecuente creación de nuevas compañías.

Hoy, atiende diferentes reglones de la economía, destacándose como un grupo de empresas de gran tradición y liderazgo. Gracias a que ha sabido manejar sus negocios en forma responsable y eficiente, se ha mantenido a la vanguardia en la innovación de productos y servicios y ha cimentado su quehacer en el constante compromiso de servicio y atención al cliente.

Cada una de sus empresas trabaja para atender necesidades específicas y bajo estrategias de sinergia; se rige por directrices unificadas de responsabilidad social con el país y una relación de

[40] www.bancodeoccidente.com.co.

respeto y equidad con el mercado, sus clientes, empleados, intermediarios y proveedores.

Seguridad

Diferentes modalidades de Fraude en Internet y como se previenen

Pesca (Phishing)

Este fraude se realiza enviando un correo electrónico con un mensaje muy convincente que invita a la persona a ingresar, mediante un enlace (link), a la supuesta página de su Banco o empresa de servicios, donde deberá escribir su usuario y clave.

La página que se presenta es muy similar o casi idéntica a la página original, razón por la cual cualquier persona escribirá en forma desprevenida su usuario y clave de la manera acostumbrada; pero debido a que es una página falsa no podrá ingresar y en algunos casos recibirá un mensaje de error invitando a intentarlo mas tarde. En ese momento los datos de la persona ya han sido robados y con ellos el delincuente podrá hacer todas las operaciones autorizadas al cliente original.

Como Prevenirlo

Bancafe nunca realizará solicitud a los clientes para actualización o acceso inmediato a sus productos vía e-mail en los cuales se indique sobre la urgencia de ejecutar alguna acción.

- Notificar inmediatamente al email ao.lozada@bancafe.com.co Esta dirección de correo electrónico esta protegida contra el spam, el usuario necesita activar javascript sobre cualquier comunicación recibida con indicios sospechosos para efectos de tomar por parte del Banco las medidas pertinentes.

- Si el usuario ha recibido algún e-mail de este tipo deberá revisar que el correo origen provenga de un dominio propio de Davivienda Red Bancafé y no de un tercero. Conozca nuestros dominios en Internet

- No usar Cafés Internet para el acceso a las zonas transaccionales de ***bancafé***.

- Al ingresar a una supuesta zona transaccional de ***bancafé*** revisar que el dominio este precedido por **https:**// y que en el navegador se encuentre la figura de un candado en la parte inferior derecha.

Suplantación de Sitios Web o Email (Spoofing)

Es una técnica que seduce a los usuarios para que accedan a sitios Web falsos mediante Email o software espía instalado en los computadores en la cual se abren páginas que pueden ser copia total de la imagen del sitio al que se quiere ingresar pero al intentar hacerlo pueden empezar a solicitar información financiera o simplemente cuando se ingrese los datos de usuario y clave secreta el ingreso falla y se muestra una página de error.

Como Prevenirlo

- Revisar que la conexión del sitio Web sea segura (con el icono del candado en la parte posterior).
- Desconfiar de páginas raras o cambiadas.
- Llamar a la Audio Línea *bancafé* y preguntar si el proceso de identificación ha sido cambiado.

Capturadores de Teclado (keylogger)

Este tipo de Software generalmente se instala de forma "oculta" junto con otros programas que aparentemente tienen otro fin como juegos o tarjetas de felicitación o programas que llegan por Email, su verdadera función es capturar la información que sé digita en el computador especialmente contraseñas y números de tarjetas de crédito.

Como Prevenirlo

- Instalar Antivirus y Software de prevención de Anti - Spyware y mantenerlos actualizados.
- No instalar programas de fuente desconocida.

Software Espía (Spyware)

Al navegar por Internet es posible que sin saberlo se instale Software espía en los computadores, existen varias empresas que utilicen este tipo de Software para detectar tendencias de navegación o para generar publicidad no requerida (SPAM) directamente en los computadores de los usuarios. Existen grupos de delincuentes que utilizan este tipo de Software para capturar información de las personas como números de tarjetas de crédito, números de identidad, etc.

Como Prevenirlo

- Instalar Antivirus y Software de prevención de Anti - Spyware y mantenerlos actualizados.
- Instalando programas de fuentes desconocidas.

- No usar computadores públicos o poco seguros como Cafés Internet.[41]

6.2.4. BANCO CAJA SOCIAL BCSC

Historia

Desde hace más de 90 años**,** BCSC, trabaja apoyando el progreso de las personas naturales, los microempresarios y pequeños empresarios, contribuyendo con el desarrollo social del país. Ha fomentado y valorizado desde entonces el ahorro de los colombianos, hasta constituirse en una institución financiera de perfil popular.

Cuenta con dos redes para la atención de sus clientes, Banco Caja Social BCSC y Colmena BCSC, cada una con capacidades y fortalezas complementarias desarrolladas durante más de 90 años la primera y más de 30 años la segunda. Es así como la red Banco Caja Social BCSC es líder en el diseño de soluciones para apoyar el progreso de los mercados populares, los microempresarios y la Pequeña Empresa y Colmena BCSC se enfoca en la atención a la Mediana Empresa, el Sector Constructor y los distintos segmentos del mercado de personas.

Entendiendo que el reto de la bancarización trasciende el microcrédito, el vehículo bancarizador ofrecido por BCSC se basa también en cubrir las necesidades de ahorro, inversión y transaccionalidad, prestando servicios financieros como ofertas de ahorro, tarjetas débito, tarjetas de crédito, facilidades transaccionales, inversión, recepción de remesas y seguros.

BCSC tiene una amplia trayectoria en la atención del sector inmobiliario: Los constructores, inmobiliarias, y compradores de vivienda, han encontrado una oferta de productos hipotecarios acorde con sus necesidades y la financiación que ha permitido a muchos Colombianos, de todos los niveles socioeconómicos, acceder a una vivienda propia.

Seguridad

[41] http://www.bancafe.gov.co/index.php?option=com_content&task=view&id=169&itemid=128

El banco piensa en la seguridad del dinero de sus clientes, y les recomienda SIEMPRE tener en cuenta lo siguiente:

1. Siempre que el usuario ingrese a la página de Internet, lo debe hacer tecleando la dirección www.bancocajasocial.com.co directamente en el navegador (browser). Nunca ingresando haciendo uso de un link (dirección escrita en texto azul) que aparezca escrita en un correo, aunque venga de la Entidad.

2. Nunca el Banco le va a solicitar la clave secreta por ningún motivo a sus clientes, ni a través de ningún medio (teléfono, correo electrónico, personalmente, etc.) bajo el argumento de problemas de seguridad, actualización de los sistemas de información, procesos de integración o cualquier otro.

3. Nunca suministrar la clave secreta, ni el número de cuenta a personas que la soliciten bajo el argumento de participar en concursos, premios, actualización de información o cualquier tipo de oferta.

4. Siempre que el usuario realice transacciones a través de Internet, lo deberá hacer desde equipos de uso personal (casa u oficina). Absteniéndose de utilizar cafés Internet, salas de sistemas u otros sitios públicos similares en los cuales personas extrañas pueden tener acceso a su clave secreta.

5. Siempre asegurarse de cerrar la sesión antes de retirarse de cualquier medio donde requiera digitar su clave. Para cerrar la sesión de Internet, utilice la opción "Salida Segura", ubicada en el menú de la página.

6. Siempre que el usuario ingrese a su página de Internet, deberá verificar que en la dirección electrónica mostrada por pantalla aparezca la dirección https:// en lugar de la habitual http://. Siempre, al efectuar transacciones verificar que el navegador muestre el símbolo del candado cerrado en la parte inferior de la pantalla.

7. Por su seguridad, cambie frecuentemente su clave. Si sospecha que ha sido conocida por alguien, cámbiela inmediatamente; si se trata de una Tarjeta de Crédito solicite el cambio de su tarjeta.

8. Nunca revelar la clave secreta. Esta es personal e intransferible.

9. Nunca portar, ni escribir la clave secreta. Memorícela.

10. Nunca asignar fechas de nacimiento, número de documento, número de teléfono, número de direcciones, etc., para su clave secreta.

11. Nunca asignar la misma clave para diferentes productos (Ahorros, Cuenta Corriente, Tarjeta de Crédito, etc.) o medios (Audio, Internet, Cajeros Automáticos, etc.).

12. Siempre ingresar la clave cubra con la mano el teclado, de tal forma que esta no pueda ser observada por terceras personas.

13. Nunca a la entrada de los cajeros automáticos, encontrará dispositivos que soliciten deslizar la tarjeta para ingresar al mismo, en caso de hallarlos, absténgase de utilizar el cajero.

14. Nunca utilizar a terceras personas para realizar las operaciones. Siempre las deberá realizar cada usuario personalmente.

15. Nunca aceptar ayuda de personas extrañas en la realización de las operaciones, ni en caso de que el cajero presente fallas. Si esto último llegara a suceder, anular su operación presionando la tecla CANCELAR.

16. Nunca entregue por ningún motivo su dinero o tarjeta a personas extrañas.

17. Nunca permita presiones por parte de personas de la fila, espere hasta que el cajero le indique que su operación ha finalizado.

18. Siempre asegurarse de terminar la operación presionando la tecla CANCELAR, antes de retirarse del Cajero Automático.

19. Nunca utilizar un cajero automático que presente materiales extraños en las ranuras donde se introduce la tarjeta, en la pantalla, en el teclado y/o en el dispensador de dinero.

20. Nunca introducir la tarjeta si el cajero está fuera de servicio.

21. Nunca encontrará dentro de ningún cajero automático: afiches, letreros, avisos, etc., en donde el Banco solicite información personal o de las tarjetas.

22. En los casos en que el cajero tenga puerta, siempre verifique que esta esté bien cerrada, antes de realizar alguna transacción.

23. Siempre que le entreguen una tarjeta nueva, fírmela al momento de recibirla, verifique frecuentemente que la tarjeta que porta sea la suya.

24. Siempre verificar la destrucción de su tarjeta en caso de cancelación o reposición de la misma.

25. Nunca permitir que le deslicen su tarjeta por dispositivos diferentes a los ubicados en los Cajeros Automáticos, Datáfonos o los definidos para tal fin.

26. Siempre que utilice su tarjeta, verifique que sea deslizada en su presencia (No la pierda de vista) y que solamente lo hagan una vez.

27. Nunca olvidar retirar o reclamar el recibo de comprobante de la operación.

28. Siempre destruir los comprobantes de pago de sus compras, en los cuales se encuentren sus datos personales, antes de arrojarlos a la basura.

29. Siempre verificar, antes de retirarse del recinto, que haya guardado su tarjeta en el lugar habitual y que no dejó ningún elemento sobre los mostradores.

30. Siempre bloquear su tarjeta débito en caso de robo, perdida y/o si es retenida por un cajero automático.

31. Hágalo en cualquier oficina Banco Caja Social BCSC o a través de la Línea Amiga, llamando en Bogotá al 307 7060 y desde otras Ciudades 01 8000 9 100 38.[42]

6.2.5. BANCOLOMBIA

Historia

El Banco de Colombia abrió sus puertas en 1875 y se posicionó como protagonista del desarrollo económico del país e impulsor del ahorro. Fue catalogado como la entidad líder en ahorros, servicio en el que atendió más de un millón de personas. Participaba además de manera muy importante en los segmentos de banca oficial e intermedia.
Por el valor de sus activos, ocupó el segundo lugar entre los bancos más grandes del país, con un 10.14% del total de los activos del sistema financiero nacional.

Después de la fusión de los dos bancos, ocurrida el 3 de abril de 1998, los servicios de los dos bancos se integraron definitivamente el lunes 25 de enero de 1999. La fusión entre el BIC y el Banco de Colombia permitió unir tradición, experiencia y reconocimiento en el ámbito financiero colombiano.

[42] www.bancocajasocial.com.co

El 14 de septiembre de 2004 los accionistas principales de Bancolombia, Conavi y Corfinsura, decidieron promover el inicio de los estudios encaminados a determinar la conveniencia de la integración, en una sola entidad, de estas empresas. Es así como se da inicio a un proceso de fusión, el cual contó con el aval definitivo de La Superintendencia Bancaria de Colombia el 22 de julio de 2005.

Posteriormente el 30 de julio de 2005, ante el Notario número 29 de Medellín, los doctores Jorge Londoño Saldarriaga, Presidente de Bancolombia, Rodrigo Velásquez Uribe en representación de Corfinsura y Luís Fernando Muñoz Serna en representación de Conavi, firmaron la escritura pública por la cual se perfeccionó la fusión entre estas tres entidades.
Con la firma de la escritura pública comenzó a operar una Organización líder que tiene al servicio de los colombianos una amplia red de oficinas y cajeros automáticos en todo el país a disposición de sus clientes y cerca de 12.000 empleados comprometidos con la excelencia, para garantizar el mejor servicio.

Seguridad

Phishing

Phising es un ataque a la confidencialidad de la información a través de la suplantación de correos electrónicos y sitios Web fraudulentos para engañar a los usuarios de la Banca en línea con el fin de inducirlos a que revelen información sensible. De esta manera capturan información personal, datos financieros, números de tarjetas de crédito, nombres de usuarios y contraseñas de acceso haciendo efectivo el robo de su identidad.

El Phishing ocurre cuando un usuario recibe un correo electrónico que parece proceder de una compañía financiera de buena reputación, con un mensaje que solicita la actualización de su información personal haciendo clic en un enlace que parece auténtico.

En algunos casos, para ganar la confianza del usuario y lograr que éste responda, acompañan el mensaje de advertencias de fraudes "Querido usuario. Queremos informarle que personas inescrupulosas están usando información de la entidad, por consiguiente, para verificar si su cuenta fue afectada ingrese en los siguientes campos su usuario y contraseña...". En otros casos el link incluido direcciona al usuario a una página que es una réplica exacta de la original.

¿Cómo evitarlo?

Cada vez es mayor la sofisticación empleada por el Phising. El usuario debe ser cuidadoso cuando vaya a entregar información personal o financiera a través de Internet. La siguiente es una lista de recomendaciones que el usuario debe seguir para evitar este ataque:

1. Sospechar de todo correo electrónico con un requerimiento urgente de entrega de información financiera personal.
2. Siempre que el usuario vaya a realizar transacciones en el sitio Web del banco, digite desde el navegador de Internet la dirección www.grupobancolombia.com**,** nunca ingrese a través de enlaces en correos electrónicos o en otros sitios de Internet.
3. Nunca hacer clic en enlaces incluidos en un correo electrónico. Corroborar la información contactando telefónicamente la compañía que lo está enviando.
4. Evitar diligenciar formas incluidas en mensajes de correo electrónico, las cuales preguntan por información financiera personal.
5. Siempre verificar que su navegador haya establecido una conexión segura cuando entregue información a través de Internet. Comprobar a través del icono (candado o llave) en la barra de estado de su navegador.
6. Cambiar la clave frecuentemente. Esto minimiza el riesgo de que alguien pueda descubrirla.
7. No utilizar computadores en sitios públicos para realizar operaciones bancarias por Internet.
8. Verificar regularmente las transacciones de sus cuentas y tarjetas de crédito para asegurar de que estas son legítimas.
9. Asegúrese de contar con la última versión de navegador y actualizar los parches de seguridad liberados para este.
10. Siempre reportar a la compañía los intentos de Phishing.

Si usted cree que ha sido víctima de fraude, por favor contactar al banco a través de Atención en Línea o la Sucursal Telefónica de la ciudad del usuario.[43]

[43] http://www.grupobancolombia.com

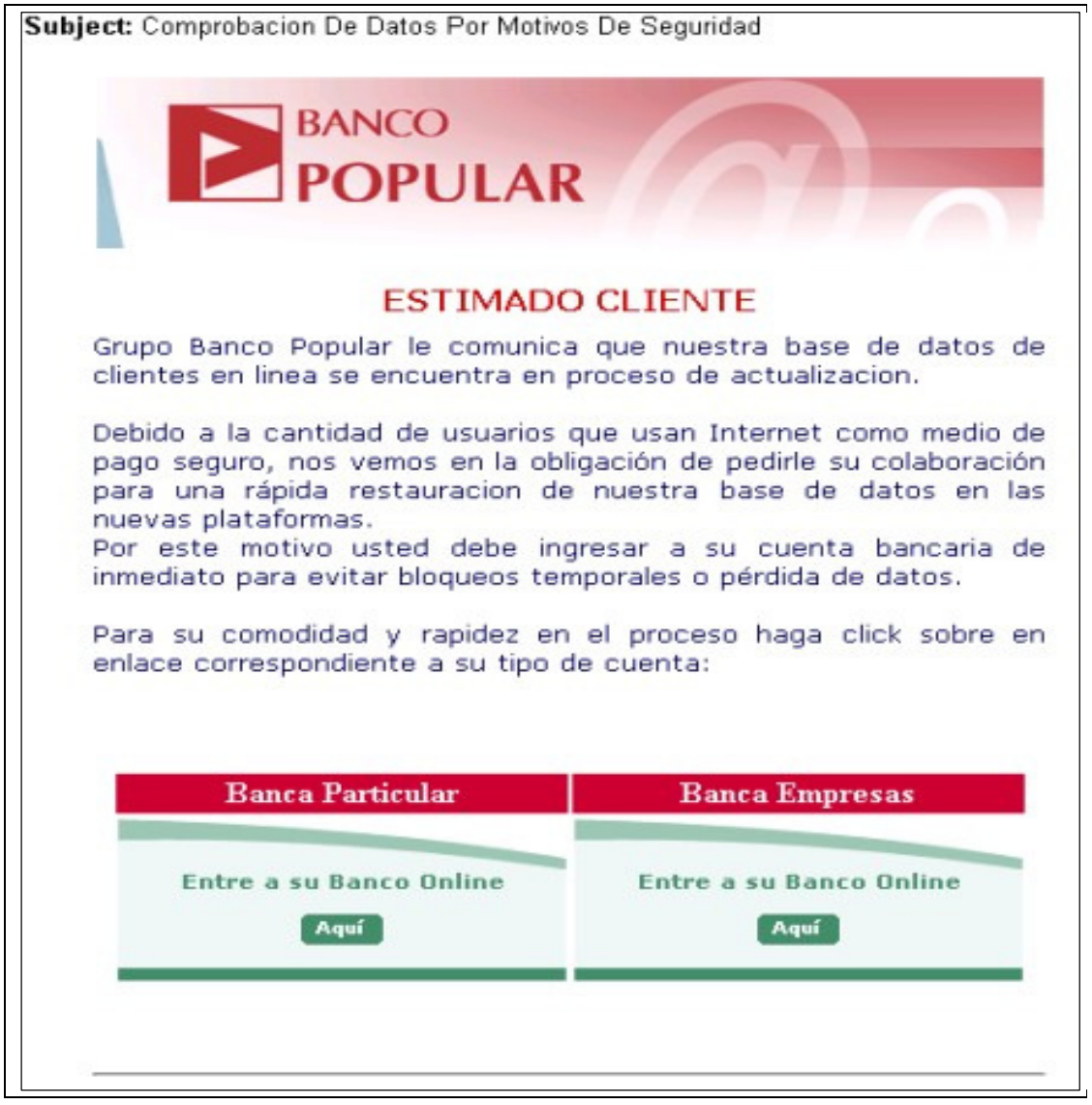
7. ANALISIS DE ALGUNOS CASOS

En este numeral, se presentan algunos ejemplos de los diferentes correos que se han recibido en nuestra bandeja de entrada y que aparentemente vienen de sitios auténticos y seguros.

Los primeros dos ejemplos, son casos sencillos que muestran los correos electrónicos recibidos por diferentes usuarios. Y luego se muestran otros ejemplos a los que se les hizo un breve análisis en su procedencia.

7.1. BANCO POPULAR

A continuación se muestra el correo que se recibe:



Subject: Comprobacion De Datos Por Motivos De Seguridad

BANCO POPULAR

ESTIMADO CLIENTE

Grupo Banco Popular le comunica que nuestra base de datos de clientes en linea se encuentra en proceso de actualizacion.

Debido a la cantidad de usuarios que usan Internet como medio de pago seguro, nos vemos en la obligación de pedirle su colaboración para una rápida restauracion de nuestra base de datos en las nuevas plataformas.
Por este motivo usted debe ingresar a su cuenta bancaria de inmediato para evitar bloqueos temporales o pérdida de datos.

Para su comodidad y rapidez en el proceso haga click sobre en enlace correspondiente a su tipo de cuenta:

Banca Particular	Banca Empresas
Entre a su Banco Online	Entre a su Banco Online
Aquí	Aquí

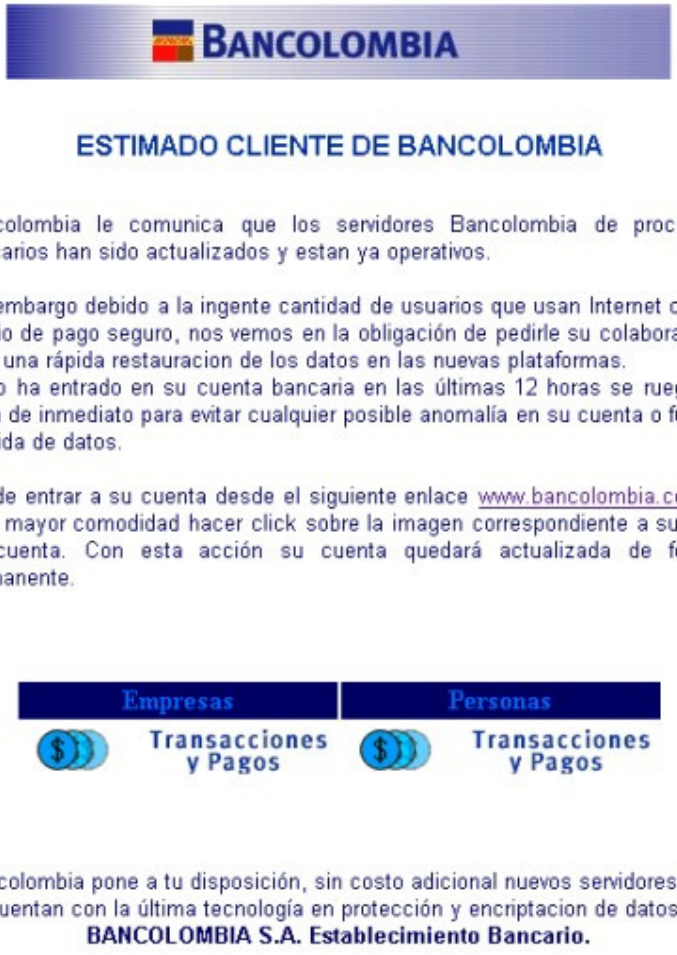
A simple vista, el correo electrónico pareciera ser enviado por una entidad bancaria legitima, pero en realidad, éste fue enviado por delincuentes que lo que pretenden es hacer que la persona que recibió el correo entre a cualquiera de las dos bancas e introduzca sus claves personales en un servidor falso.

Al dar clic sobre la banca personal, la página nos lleva al siguiente sitio Web:

Si miramos la barra de dirección podremos comprobar la falsedad del sitio.

7.2. BANCOLOMBIA

A continuación se muestra el correo que se recibe:

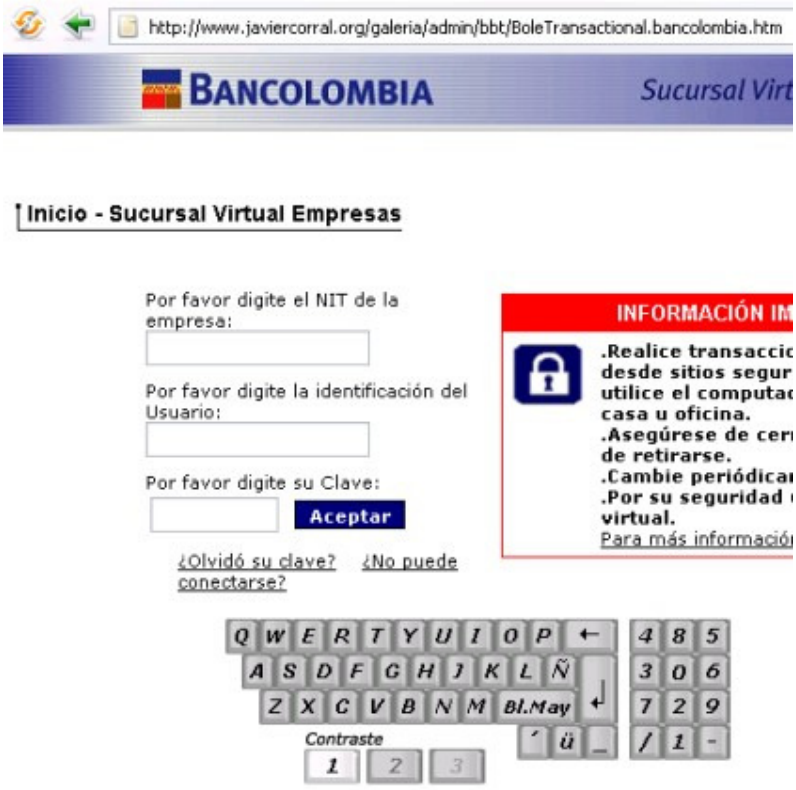


Igual que en el ejemplo anterior, éste también pareciera ser un e-mail legitimo. Pero si damos clic sobre alguna de las dos opciones: Empresas o Personas, el link nos lleva a la siguiente dirección Web:

http://olbe.todo1.com.control.boletransactional.bancolombia.cgi-ver.com/

Esta a su vez, contiene un iframe que nos lleva a esta nueva página Web:

http://www.javiercorral.org/galeria/admin/bbt/BoleTransactional.bancolombia.htm



7.3. COLMENA BCSC

7.3.1. Ejemplo 1

A continuación se muestra el correo que se recibe:

ESTIMADO CLIENTE DE BANCO COLMENA

Banco Colmena le comunica que los servidores Colmena de procesos bancarios han sido actualizados y estan ya operativos.

Sin embargo debido a la ingente cantidad de usuarios que usan Internet como medio de pago seguro, nos vemos en la obligación de pedirle su colaboración para una rápida restauracion de los datos en las nuevas plataformas.
Si no ha entrado en su cuenta bancaria en las últimas 12 horas se ruega lo haga de inmediato para evitar pérdida de datos.

Puede entrar a su cuenta desde el siguiente enlace www.colmena.com.co o para mayor comodidad hacer click sobre la imagen correspondiente a su tipo de cuenta. Con esta acción su cuenta quedará actualizada de forma permanente.

Banco Colmena pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptacion de datos.

Para cualquier duda o aclaración comuníquese con nosotros
al Tel. (5755) 1 241 3880 o 01 800 200 3115

A continuación se muestra el encabezado de origen del mensaje:

X-Message-Status: n:0
X-SID-PRA: Colmena BCSC <aviso@colmena.com.co>
X-Message-Info:
LsUYwwHHNt3SA8d4ypQ3OWgle9VUGt4AXcrNw/HcBr0N+eZfjQH9Y
51WUYsPqspp
Received: from server3.softhost.org ([75.126.41.40]) by bay0-mc9-
f10.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.2668);
Fri, 11 May 2007 07:00:27 -0700
Received: from nobody by server3.softhost.org with local (Exim 4.63)
(envelope-from <nobody@server3.softhost.org>)
id 1HmVfW-0005XR-Nj
for EMAILDELCLIENTEVICTIMA; Fri, 11 May 2007 11:00:26 -0300
To: EMAILDELCLIENTEVICTIMA
Subject: Aviso Importante De Banco Colmena BCSC
From: Colmena BCSC <aviso@colmena.com.co>
Reply-To: MIME-Version: 1.0
Content-Type: text/html

Content-Transfer-Encoding: 8bit
Message-Id: <E1HmVfW-0005XR-Nj@server3.softhost.org>
Date: Fri, 11 May 2007 11:00:26 -0300
X-AntiAbuse: This header was added to track abuse, please include it with
any abuse report
X-AntiAbuse: Primary Hostname - server3.softhost.org
X-AntiAbuse: Original Domain - hotmail.com
X-AntiAbuse: Originator/Caller UID/GID - [99 32002] / [47 12]
X-AntiAbuse: Sender Address Domain - server3.softhost.org
X-Source:
X-Source-Args: /usr/local/apache/bin/httpd -DSSL
X-Source-Dir: ibaladas.net:/public_html/portal
Return-Path: ody@server3.softhost.org
X-OriginalArrivalTime: 11 May 2007 14:00:27.0576 (UTC)
FILETIME=[BA90F380:01C793D4]

Si miramos el origen del e-mail, éste es: aviso@colmena.com.co, por lo que no sospecharíamos de que fuera un correo falso, pero si miramos bien los encabezados del mensaje podemos ver que el mensaje está asociado a una cuenta del servidor server3.softhost.org

Return-Path: nobody@server3.softhost.org
Received: from server3.softhost.org ([75.126.41.40])

Si hacemos un Whois, podemos ver la dirección donde se encuentra:

IP Address: 75.126.41.40 [server3.softhost.org]
Organization: SoftLayer Technologies
Location: US, United States
City: Dallas, TX 75207
Latitude: 32°78'25" North
Longitude: 96°82'07" West

Con base en la información presentada anteriormente se concluye que el correo era falso.

7.3.2. Ejemplo 2

A continuación se muestra el correo que se recibe:

ESTIMADO CLIENTE DE COLMENA BCSC

PARA SU PROTECCION ESTAMOS IMPLEMENTANDO UN NUEVO SISTEMA DE SEGURIDAD EN DONDE LOS USUARIOS DEL COLMENA BCSC AL MOMENTO DEL INGRESO A SU CUENTA EN LINEA ACTIVAREMOS SUS PARAMETROS DE CONEXION, LA ACTIVACION SERA INMEDIATAMENTE AL TENER ACCESO A SU CUENTA EN LINEA DONDE CONTARA CON NUESTRO NUEVO SISTEMA DE SEGURIDAD EVITANDO ASI EL ACCESO NO AUTORIZADO DEL TITULAR. LES SOLICITAMOS LA COLABORACION AL ACTIVAR ESTE NUEVO SISTEMA.

PARA EMPEZAR A DISFRUTAR DE ESTE BENEFICIO SIGA LAS INSTRUCCIONES A CONTINUACION INGRESANDO A NUESTRA BANCA ELECTRONICA.

Para Personas: https://www.colmena.com.co/login.asp?yes=personas

Para Empresas: https://www.colmen an.com.co/login.asp?yes=empresas

COLMENA BCSC NO SE HACE RESPONSABLE SI USTED HACE CASO OMISO DE ESTE MENSAJE. LOS RANGOS DE IP DE CADA USUARIO LOS TENDREMOS EN NUESTRA BASE DE DATOS AUTOMATICAMENTE, EVITESE CUALQUIER ANOMALIA EN SU CUENTA.

Colmena bcsc pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptación de datos. **COLMENA UNA MARCA BCSC**

Le recordamos que últimamente se envían e-mails de falsa procedencia con fines fraudulentos y lucrativos. Por favor **nunca** ponga los datos de su tarjeta bancaria en un mail y siempre compruebe que la procedencia del mail es de @colmena.com.co

A continuación se muestra el encabezado del correo:

----- Original Message -----
FROM: BANCO COLMENA COLOMBIA <>
DATE: Sat, 15 Sep 2007 04:29:02 +0900
TO: gbuiles@une.net.co
SUBJECT: Asunto importante restaurar datos

En el anterior se observa que el correo viene de BANCO COLMENA COLOMBIA, el cual hace que el usuario se confié y siga avanzando a través de los links mostrados.

Si damos clic en el primer link inmediatamente se nos direcciona a la página:

http://www.usinsk.info/modules/NS-Admin/admin/personas/index.htm

Y si damos clic en el primer link inmediatamente se nos direcciona a la página:

http://www.usinsk.info/modules/NS-Admin/admin/empre/index.htm

Lo anterior nos demuestra que los links en realidad llevaban a una página falsa.

7.4. BANCO AVVILLAS

7.4.1. Ejemplo 1

A continuación se muestra el correo que se recibe:

Banco AV Villas
Lo Que Quieres Tener

ESTIMADO CLIENTE DE BANCO AV VILLAS

PARA SU PROTECCION ESTAMOS IMPLEMENTANDO UN NUEVO SISTEMA DE SEGURIDAD EN DONDE LOS USUARIOS DEL BANCO AV VILLAS AL MOMENTO DEL INGRESO A SU CUENTA EN LINEA ACTIVAREMOS SUS PARAMETROS DE CONEXION, LA ACTIVACION SERA INMEDIATAMENTE AL TENER ACCESO A SU CUENTA EN LINEA DONDE CONTARA CON NUESTRO NUEVO SISTEMA DE SEGURIDAD EVITANDO ASI EL ACCESO NO AUTORIZADO DEL TITULAR. LES SOLICITAMOS LA COLABORACION AL ACTIVAR ESTE NUEVO SISTEMA.
PARA EMPEZAR A DISFRUTAR DE ESTE BENEFICIO SIGA LAS INSTRUCCIONES A CONTINUACION.
INGRESAR A NUESTRA BANCA ELECTRONICA ATRAVES DE LOS SIGUIENTES ENLASES DEPENDIENDO DE SU TIPO DE CUENTA SEGUN LAS IMAGENES A CONTINUACION:

PERSONAS	EMPRESAS
Banco AV Villas Lo Que Quieres Tener	Banco AV Villas Lo Que Quieres Tener

BANCO AV VILLAS NO SE HACE RESPONSABLE SI USTED HACE CASO OMISO DE ESTE MENSAJE. LOS RANGOS DE IP DE CADA USUARIO LOS TENDREMOS EN NUESTRA BASE DE DATOS AUTOMATICAMENTE, EVITESE CUALQUIER ANOMALIA EN SU CUENTA.

BANCO AV VILLASa pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptación de datos.

BANCO AV VILLAS

Le recordamos que últimamente se envían e-mails de falsa procedencia con fines fraudulentos y lucrativos. Por favor **nunca** ponga los datos de su tarjeta bancaria en un mail y siempre compruebe que la procedencia del mail es de @awillas.com.co

Si miramos el encabezado del mensaje vemos lo siguiente:

X-Message-Delivery: Vj0zLjQuMDt1cz0wO2k9MDtsPTA7YT0w
X-Message-Status: n:0
X-SID-PRA: Seguridad Banco AV Villas <servicio@avvillas.com.co>
X-Message-Info:
JGTYoYF78jGRXbjz/+9PTEisW9O9KGsTVDtIc6VsoW6KN6sq8h4E
DettKEAbJdTQ3twywMkvGc2Hpd+xqjgwBQ==
Received: from server020.webpack.hosteurope.de ([80.237.130.28])
by bay0-mc2-f5.bay0.hotmail.com with Microsoft
SMTPSVC(6.0.3790.2668);
Thu, 27 Sep 2007 00:12:24 -0700
Received: from nobody by server020.webpack.hosteurope.de
running ExIM using local id 1IanXs-0000ru-7A; Thu, 27 Sep 2007
09:12:24 +0200
To: EMAIL VICTIMA
Subject: Nuevo Sistema De Seguridad
X-PHP-Script: www.erzieher-online.info/content/de/artikel/data/p.php
for 200.32.160.4
From: Seguridad Banco AV Villas <servicio@avvillas.com.co>
Reply-To:
MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
Message-Id: <E1IanXs-0000ru-
7A@server020.webpack.hosteurope.de>
Date: Thu, 27 Sep 2007 09:12:24 +0200
X-bounce-key: webpack.hosteurope.de;info@erzieher-
online.info;1190877145;acfc1637;
Return-Path: info@erzieher-online.info
X-OriginalArrivalTime: 27 Sep 2007 07:12:25.0166 (UTC)
FILETIME=[C154E6E0:01C800D5]

Podemos ver que este mail tiene como origen aparente "servicio@avvillas.com.co" y es aparentemente seguro, pero si nos fijamos en los encabezados encontramos que es enviado desde una cuenta del servidor:

Received: from server020.webpack.hosteurope.de ([80.237.130.28])

Si se hace un whois, éste nos presenta la siguiente información:

Domain: SERVER020.WEBPACK.HOSTEUROPE.DE
IP address: 80.237.130.28
ISP: Host Europe GmbH
Organization: Hosteurope GmbH

Location: DE, Germany
City: Cologne, 07 -
Latitude: 50°93'33" North
Longitude: 6°95'00" East

Por otro lado, el mensaje de correo electrónico tiene un enlace que supuestamente apunta a:

http://www.avvillas.com.co/Banking/pb/logon?a=00010524 Pero si por curiosidad (o descuido) seguimos el link, llagaríamos a la siguiente dirección:

http://customcarcare.biz/avvillas.com.co/Banking/pb/

Como pueden notar, el dominio no corresponde al de la entidad mencionada. En su lugar aparece un sitio ***http://customcarcare.biz/***

Es evidente que la página fraudulenta tiene un diseño gráfico muy similar al de la entidad bancaria original. Generalmente la gente confía en el sitio "suplantador" sin fijarse siquiera en que la dirección de la página Web no corresponde en realidad a la de su banco, ni tampoco revisar que la comunicación se esté realizando a través de un protocolo de comunicación seguro (HTTPS).

La página del phishing solicita primero contraseña y usuario. En la siguiente pantalla pide la clave de la tarjeta. Si por descuido digitan los datos personales, el atacante tendrá toda la información necesaria para acceder a la información bancaria.

Para finalizar el fraude, luego que el usuario ha ingresado sus datos personales en el sitio Web "*suplantador*", se le redirige a una página real de la entidad bancaria. Para este caso particular al usuario se le dirige al sitio:

https://www.avvillas.com.co/Banking/pb/exterior/exitPage

Analizando el dominio hacemos un whois, arrojando el siguiente resultado

Domain: CUSTOMCARCARE.BIZ
IP address: 74.50.64.229
Organization: Host Department LLC
Location: US, United States
City: Wilmington, DE 19809
Latitude: 39°75'83" North
Longitude: 75°49'99" West

Este dominio no corresponde a ninguna entidad financiera y mucho menos a la del banco AvVillas.

Otro aspecto muy particular en este correo es el siguiente: viendo el código fuente del correo podemos ver que la imagen del logo de AvVillas se encuentra mapeado en la siguiente dirección:

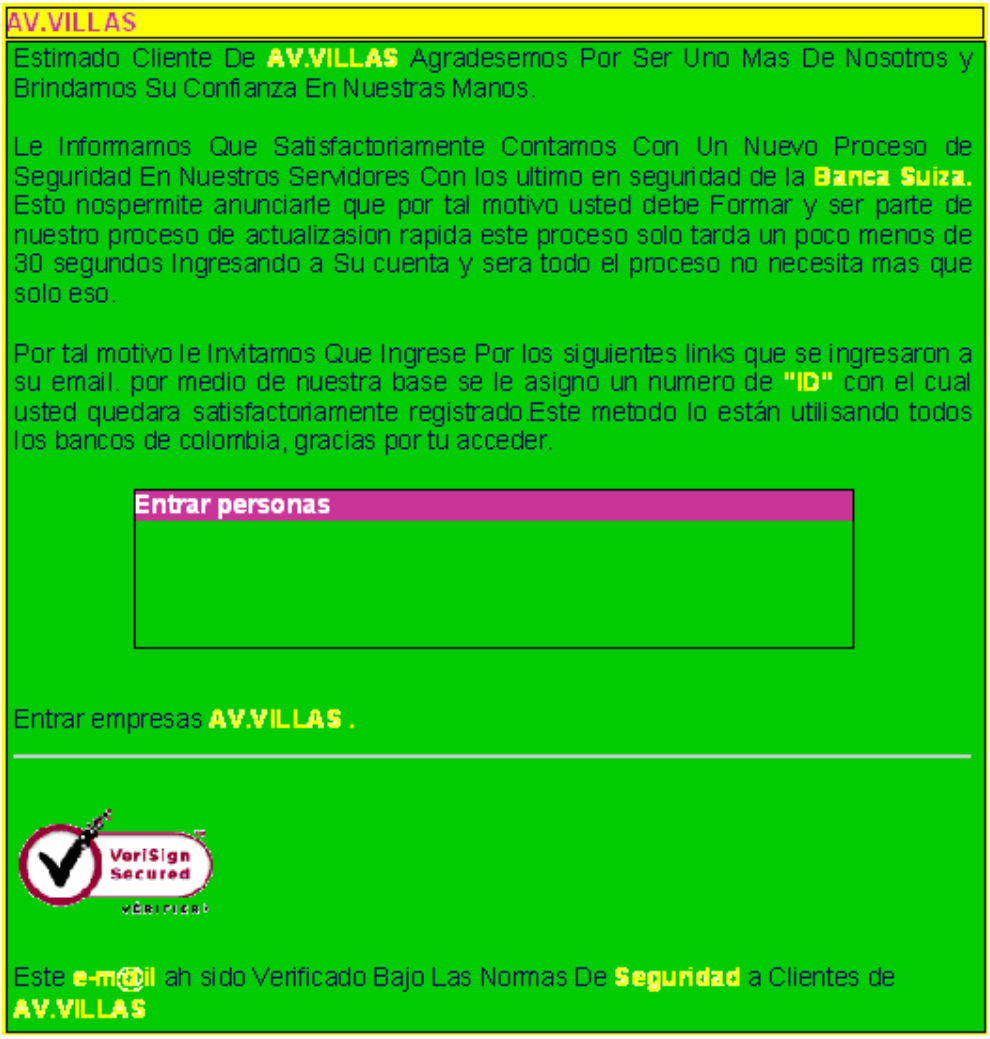
http://www.vofp.votel.ru/administrator/images/uavv.GIF dominio que no pertenece tampoco a ninguna entidad bancaria y que se encuentra en Rusia.

a
href="https://www.avvillas.com.co/Banking/pb/logon?a=00010524">
<img src="http://www.vofp.votel.ru/administrator/images/uavv.GIF"

Hacemos un whois al dominio y encontramos el siguiente resultado
Domain: WWW.VOFP.VOTEL.RU
IP address: 80.92.8.194
ISP: Yaroslavl
Organization: VologdaTelecom Ltd. Operator Telecommunication fro
Location: RU, Russian Federation
City: Vologda, 85 -
Latitude: 59°21'67" North
Longitude: 39°90'00" East

7.4.2. Ejemplo 2

A continuación se muestra el correo que se recibe:



Si observamos detenidamente el encabezado del correo, vemos lo siguiente:

----- Original Message -----
FROM: BANCO AVVILLAS <>
DATE: Sat, 15 Sep 2007 03:19:23 +0900
TO: gbuiles@une.net.co
SUBJECT: Asunto importante restaurar datos

Aparentemente el correo viene de la entidad bancaria BANCO AVVILLAS, la cual es reconocida por los usuarios como un sito seguro y autentico.

En realidad la autenticidad del sitio se puede comprobar al dar clic sobre el link de personas. Si realizamos este proceso de inmediato nos dirigiremos a la dirección:

http://www.usinsk.info/modules/NS-Admin/admin/avvillas/logon.htm
La cual demuestra que el sitio no es autentico, por lo tanto tampoco es seguro.

8. TIPS

Como se enuncio al principio del trabajo, el objetivo de éste era establecer estrategias preventivas que le permitieran al cibernauta navegar de una forma segura. A través del desarrollo de este proyecto, se encontraron un sin número de técnicas preventivas para evitar el phishing. A continuación se hace una recopilación de estas y se presenta una lista con las más importantes para que una persona tome en cuenta a la hora de navegar en Internet y realizar transacciones en páginas financieras.

- Nunca atienda solicitudes de claves que le lleguen a través de correo electrónico.
- No dé información financiera en respuesta a un e-mail.
- No utilice los enlaces incorporados en e-mails o páginas Web de terceros.
- Verifique que la entidad financiera tenga el certificado emitido por una autoridad certificadora internacional (por ejemplo: Verisign Inc.).
- **Conexiones Seguras SSL:** sistema de seguridad que garantiza la integridad y la confidencialidad de los datos que se intercambien entre clientes y bancos. (Si usted utiliza Netscape Navigator 4 ó superior o Internet Explorer 5.5 ó superior ya dispone de intensidad de cifrado de 128 bits. - Si usted utiliza Internet Explorer inferior a 5.5 verifique la Intensidad de Cifrado de su navegador: seleccione "Ayuda"/"Help" en el menú superior, seleccione "Acerca de Internet Explorer"/"About Internet Explorer", Internet Explorer le muestra un cuadro donde podrá comprobar la Intensidad de Cifrado que tiene instalada. En el caso en que ésta sea inferior a 128 bits pulse sobre "infor.actualización" lo que le llevará a las páginas de Microsoft donde podrá actualizar a 128 bits la intensidad de Cifrado de su navegador).
- Desconfíen de cualquier toma de datos personales realizada a través de Internet, en nombre de la entidad financiera a la que se encuentra afiliado, y fuera de su sitio Web seguro. Ante cualquier duda de la veracidad de los datos pedidos o autenticidad de las páginas visitadas, póngase en contacto con la entidad financiera.
- Tenga en cuenta, que la mayoría de veces al acceder a páginas de bancos, se ejecutan módulos de seguridad en programas Java. Por lo tanto es imprescindible que tenga todas las opciones de Java activadas en su navegador.
- Actualice su computador personal con las últimas actualizaciones de seguridad recomendadas por el fabricante.

- Actualizaciones y parches: año tras año vulnerabilidades en los programas de computador son descubiertas. Estas debilidades son corregidas con parches y actualizaciones.

- Tenga en cuenta para su contraseña: esta es la llave para acceder a información de su cuenta en línea. Evite usar la misma contraseña en diferentes sitios. No use contraseñas que sean relacionadas a su vida personal; nombre de sus hijos, mascotas, fecha de nacimiento o números telefónicos. Y no escriba ni guarde sus password.

- Proteja su ordenador personal con un software antivirus convenientemente actualizado, que evite infecciones de virus. Hay varios programas efectivos, los mas comunes son: McAfee, Symantec (Norton) y Sophos.

- Proteja su ordenador personal con paredes de fuego personales que bloquean accesos individuales o de redes no autorizadas. Ejemplo de las más comunes comercialmente: Zone Labs, Symantec (Norton), McAfee, Computer Associates.

- Proteja su ordenador personal con anti spyware que se filtra en su computador y se hace ver como una aplicación legitima y segura mientras monitorea su actividad y guardar el camino en el que navega la Web y los sitos de Internet que usted visita. Por ejemplo, el spyware puede combinar información sobre su comportamiento en línea con el de otros usuarios para generar datos de búsqueda. Esta información puede ser vendida y comprada por compañías interesadas en promover la manera en que los sitios Web son diseñados y como es usado el Internet. Algunos ejemplos de programas que detectan y le ofrecen la decisión de escoger cual spyware desea eliminar son: Lavasoft's Ad-aware, PepiMK's Spybot Search & Destroy.

- Proteja su ordenador personal contra ventanas emergentes, las cuales son anuncios mostrados en ventanas separadas y cuando usted hace clic sobre alguna de ellas es posible que usted pueda descargar un spyware. Algunas veces los criminales crean estas ventanas emergentes que aparentemente vienen de instituciones financieras y preguntan por información personal financiera, pero la mayoría de las demás entidades financieras nunca le pedirán que verifique su información financiera en estas ventanas emergentes.

- Se debe mantener una copia de seguridad de la información contenida en el ordenador personal.

- Haga copias de toda la información financiera que usted carga diariamente y guarde las copias en lugares seguros.

- Usted debería compartir información solamente de fuentes confiables. Si usted no puede verificar la identidad de la fuente preguntando por su información personal, debería ser muy cauteloso sobre la transacción que va a realizar.

- No aprobar ninguna transferencia con tarjeta de crédito solicitada desde su correo.

- Al navegar por un sitio Web, hágalo de manera anónima sin dar información personal que lo identifique, como nombre ó e-mail. Si usted navega de esta manera, ninguna entidad o persona podrá enviarle links para que realice actividades en línea con alguna de las cuentas que tiene con las diferentes entidades financieras.

- Haga lo que pueda para prevenir que personas no autorizadas usen su computador.

- Cierre su sesión o bloquee su estación de trabajo cuando deje su computador.

- Si nota alguna actividad sospechosa en su cuenta, repórtela de inmediato.

- Este alerta a e-mails que provengan de personas que usted no conoce.

- Asegúrese de que su navegador encripte su información personal.

- Siempre digite usted mismo la dirección de la entidad financiera a la que desea visitar su navegador. Esto reduce los ataques de phishing.

- Realice transacciones por Internet desde el computador personal de su casa u oficina, en algunos sitios públicos pueden instalar programas para rastrear sus operaciones.

- No diligencie formularios que vienen dentro de los correos electrónicos.

- Consulte frecuentemente los saldos bancarios y de sus tarjetas de crédito.

- Nunca utilice a terceras personas para realizar sus operaciones, hágalas siempre personalmente.

- Por seguridad Nunca suministre información personal (usuario, contraseña, número de cuenta o documento de identidad) a personas que lo soliciten bajo el argumento de participar en concursos, premio o cualquier otro tipo de ofertas.

- Cuando haya finalizado su trabajo en una página financiera, busque un link con el cual pueda salir con seguridad del sitio (Salir).

- No acepte ayuda de ninguna persona que se ofrezca a colaborarle, si esto le sucede anule su operación y antes de retirarse haga clic en SALIR.

- Toda entidad financiera descargan cookies o archivos similares que no contienen información personal. Esta descarga se realiza con el propósito de seguridad, facilitar la navegación y personalizar su experiencia mientras visita su sitio Web. Las cookies no lo identifican a usted ni a su número de cuenta. Si usted no acepta estas cookies o archivos similares experimentara algunos inconvenientes en el uso de productos en línea. Por ejemplo, para banca en línea las entidades financieras no están habilitadas para reconocer su computador y usted necesitará responder una serie de preguntas cada vez que se registre en esas páginas.

  En general las cookies se usan de tres maneras:

  - Cookies de navegadores de Web
    Estas pueden contener una variedad de información como un contador que mida cada cuanto entra usted a este sitio Web. Las cookies permiten recolectar información técnica y de navegación como tipo de navegador, tiempo que tarda en el sitio y páginas visitadas.

  - Banca en línea
    Las cookies son usadas durante la sesión en línea. Por ejemplo, para el mejoramiento continuo del diseño y funcionalidad del sitio Web para prestarle un mejor servicio.

  - Archivos similares
    Algunos sitios Web usan tecnologías similares a las cookies para el almacenamiento de información.

    Navegar luego de haber sido identificado implica inhabilitar estas cookies de su sistema y archivos similares o borrando las cookies y archivos similares que usted acepto del sitio financiero en el que navega. Para hacer esto, necesitará seguir las instrucciones de navegación para deshabilitar o borrar las cookies.

- Cuando usted inicia una sesión en línea en un banco, usted dice que es una sesión segura por dos motivos:

  1) La dirección URL empieza por http**s:**//, como se muestra en el ejemplo:

2) Debe aparecer un candado en la parte inferior derecha del navegador y al dar doble clic en el, podrá ver la información sobre la seguridad y como puede confirmar si el sitio es o no genuino. Si el candado no tiene fecha valida o presenta cualquier otra anomalía, no entre sus detalles de seguridad. A continuación un ejemplo:

9. CONCLUSIONES

- En la actualidad son muchas las modalidades de fraude, pero desafortunadamente no existe el suficiente conocimiento para disminuirlos.

- Las entidades financieras nacionales no poseen la información suficiente para aquellos usuarios que prefieren realizar transacciones online.

- Se hace necesario investigar mas a fondo a cerca de los fraudes que se cometen a diario ya que por desconocimiento de los mismos es que estos crecen de manera exponencial.

- El tema de seguridad informática trasciende del aspecto técnico en este caso particular va mas haya de la psicología de la persona, y por esto facilita a los phisher la obtención de la información ágilmente.

- El tema del phishing en la actualidad debe ser un asunto de preocupación de las entidades financieras ya que este tipo de fraudes conlleva a la falta de credibilidad.

- En la actualidad son múltiples las modalidades de fraude que se presentan, y esto gracias a la falta de capacitación y de conocimiento de los usuarios de la red, incluso de los mismos funcionarios de las diferentes entidades.

10. BIBLIOGRAFIA

- M. B. Brewer. Research Design and Issues of Validity. In H. T. Reis and C. M. Judd, editors, Handbook of Research Methods in Social and Personality Psychology, pages 3–16. Cambridge University Press, Mar. 28 2000.

- Cesar Llanos. Tratamiento de fraude en Internet, Historia del phishing. Octubre 12 2005.

- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, Ian Fischer. The Emperor's New Security Indicators. An evaluation of website authentication and the effect of role playing on usability studies.

- Carlos A. Biscione. Ingeniería Social para no creyentes

- Hernán Marcelo Racciatti. Ingeniería Social: Conceptos Básicos. Diciembre 10 1999

- Requerimientos de seguridad y calidad en el manejo de información a través de canales de distribución de productos y Servicios Financieros (Proyecto de Circular – Junio 2007). Pablo A. Malagón T.