



Vulnerabilidad de Phishing en Sitios Bancarios en Argentina

La creciente aceptación de nuevas tecnologías en el campo de las comunicaciones y, en particular, el explosivo crecimiento de Internet a nivel mundial, se encuentran fielmente reflejados en la aceptación y uso de los sistemas de Home Banking disponibles actualmente en el mercado argentino.

Tanto individuos como organizaciones se han visto favorecidos por la disponibilidad de servicios en línea cada vez más útiles para realizar las actividades cotidianas. Los servicios que originalmente se encontraban limitados a transferencias entre cuentas y pago de servicios propios se han extendidos con la posibilidad de efectuar transferencias a terceros, adquirir acciones, comprar o vender divisas, etc.

Sin embargo, como todo nuevo desarrollo, la actividad es susceptible a los riesgos que implica operar en redes de comunicaciones abiertas, como Internet. Aquellas instituciones que han incorporado este tipo de operaciones en el menú de servicios que ofrecen a sus clientes en línea, han sido objeto de diversos tipos de ataques para obtener acceso a cuentas que permitan realizar operaciones de manera fraudulenta. El mecanismo que mayor éxito ha tenido, denominado “phishing”, consiste en un engaño al cual es inducido el usuario real de la cuenta con el objeto de entregar sus claves de acceso a un sitio falso¹.

El presente informe se ha centrado en el análisis de uno de los aspectos que favorecen la explotación de este tipo de ataque: el diseño de los sitios de las instituciones financieras de Argentina (tanto para banca minorista como servicios a empresas). Como se podrá apreciar más adelante, el informe solamente describe porcentajes sobre el total analizado, de manera de garantizar la confidencialidad de la identidad de las instituciones analizadas². Este análisis fue realizado durante el mes de Julio de 2005.

¹ En www.antiphishing.org se puede encontrar información detallada sobre este tipo de ataque.

² Aquellos responsables de instituciones financieras de Argentina que lo deseen, pueden solicitar el detalle del análisis que le corresponde a su entidad dirigiéndose a research@certisur.com



ÍNDICE DE CONTENIDO

+ Introducción.....	3
+ Características analizadas	3
+ Ámbito de aplicación	4
Resultados Análisis Home Banking	5
Resultados Análisis Banca Electrónica.....	5
+ Errores más comunes	5

+ Introducción

El phishing es una técnica que aprovecha un conjunto de vulnerabilidades para lograr su objetivo: “obtener los datos necesarios de un usuario de tal manera de poder impersonar su identidad sobre alguno de los servicios que el legítimo usuario posee”.

Este tipo de técnica, que conjuga elementos denominados de “ingeniería social” junto con componentes tecnológicos, aprovecha alguna o varias vulnerabilidades que son intrínsecas a los sistemas de autenticación en uso actualmente por parte de las instituciones financieras, entre ellas:

1. El escaso conocimiento del usuario acerca de la tecnología que él mismo emplea no le permite distinguir entre un correo electrónico falso o verdadero. Adicionalmente no se encuentra suficientemente capacitado como para determinar si un sitio Web al que se está conectando es legítimo y pertenece efectivamente a la entidad financiera de la cual es cliente.
2. El sistema de autenticación mayoritariamente utilizado, basado en nombre de usuario y contraseña, es fácilmente “robable” por medio de esta técnica, por lo cual la identidad de un usuario se encuentra protegida básicamente por el conocimiento que el usuario tenga de los elementos de identificación previamente mencionados.
3. Los diseños utilizados por las instituciones financieras para los servicios que prestan sobre Internet no necesariamente consideran los aspectos citados, no permitiendo a los usuarios hacer uso de las signos de identidad que debe tener en cuenta para no ser objeto de un fraude de robo de identidad.

Los sitios analizados son los que corresponden a las instituciones financieras informados por el Banco Central de la República Argentina en su página Web (www.bcra.gov.ar).

Para una mejor clasificación de la información brindada en el presente estudio, se ha efectuado una diferenciación básica entre dos tipos de servicios: Home Banking, destinado a atender las operaciones de banca minorista y, en general, de administración de cuentas personales; Banca Electrónica, que comprende los servicios destinados a empresas. Es importante señalar que en este último están involucradas operaciones por valores sensiblemente superiores y, por lo tanto, en donde se concentra un riesgo mayor en caso de producirse un ataque exitoso.

+ Características analizadas

Para el presente informe se han analizado varias características que deben ser consideradas en el diseño de todo sitio en donde se requiera la identificación por parte del usuario.

Las entidades financieras no pueden impedir que sus clientes reciban un correo electrónico (primera etapa de un ataque de phishing), incitándolo a acceder a un sitio falso para aportar los datos de su identidad con las más diversas excusas. Por ello, es fundamental que las características que permiten que los usuarios identifiquen a un sitio se encuentren fácilmente accesibles.

Entre estas características podemos enumerar:

- El sitio debe poseer un certificado digital válido, emitido por una empresa que es de la confianza del usuario y que no despliegue ningún mensaje de alerta al acceder al sitio. Por otro lado, el certificado debe ser utilizado e instalado apropiadamente, es decir que el Common Name indicado en el mismo se corresponda con el sitio del banco³.

³ Un certificado digital para servidor permite la identificación del titular del sitio y, utilizando el protocolo SSL, encriptar la comunicación, de modo tal que los datos que ingrese el usuario no puedan ser accedidos por terceros no autorizados. En la medida en que el Certificado Raíz de la Autoridad Certificante emisora del certificado esté instalado en el software del usuario, ese certificado será considerado automáticamente como confiable para dicho usuario.



- Para poder observar el certificado y encriptar la comunicación el acceso al sitio debe hacerse por medio del protocolo HTTPS y no HTTP. El usuario puede verificar esta condición leyendo la barra de navegación del browser⁴. En la misma **debe** observarse el nombre completo del sitio del banco⁵.
- El símbolo de un candado aparece en la parte inferior del navegador, permitiendo al usuario determinar que se encuentra conectado con un sitio autenticado y que la comunicación se efectuará de manera encriptada⁶.
- Presionando sobre el candado, el usuario puede comprobar todos los datos contenidos en el certificado emitido a la institución por una autoridad certificante de confianza. Debería verificar que el nombre de la organización titular del certificado coincide con el nombre de su institución financiera.

Es importante destacar que las características enunciadas anteriormente se encuentran descriptas en diversos sitios, algunos de ellos correspondientes a entidades financieras, con el objeto de capacitar a sus usuarios sobre el uso apropiado de Internet y de las herramientas de seguridad disponibles.

En ocasiones, el diseño del sitio incorpora un elemento adicional muy importante que le permite al usuario acceder directamente a información brindada por la autoridad emisora del certificado del sitio y verificar su estado (válido, vencido, revocado). Este símbolo, normalmente conocido como “sello de seguridad”, no ha sido tenido en cuenta para el análisis general de vulnerabilidad, no

⁴ Un error habitual, por motivos de diseño, es abrir una página nueva para que el usuario realice sus operaciones, pero ocultando la barra de navegación, con lo cual la verificación no puede ser realizada.

⁵ Ver más adelante la observación efectuada con respecto a las instituciones que derivan al cliente a la página de otra para operar

⁶ Los errores más habituales que no permiten visualizar este símbolo son el uso de elementos no seguros (externos a la página Web en la que debe transaccionar el usuario) tales como banners sobre la misma página. Algunos sitios ocultan la barra inferior del navegador, tal como sucede con la barra de navegación.

obstante lo cual el nivel de uso del mismo puede ser observado más adelante en el presente informe.

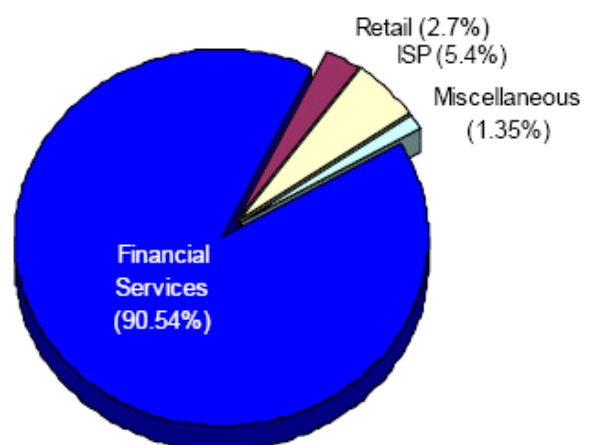
Un aspecto que no ha sido considerado como erróneo en los emergentes que se muestran a continuación es la derivación del usuario a páginas que no forman parte del sitio del Banco para realizar sus transacciones. Sin embargo, en la medida en que el usuario pueda reconocer las condiciones de seguridad del sitio con el que opera, es importante que la página Web en la que realiza todas sus transacciones esté bajo el dominio de la institución financiera de la cual es cliente. Esto le permite al cliente verificar que en la barra de direcciones de su navegador efectivamente aparece el nombre de la entidad con la que pretende operar.

+ **Ámbito de aplicación**

El presente análisis ha sido realizado sobre uno de los productos o servicios más desarrollados actualmente del sistema financiero: los servicios de HomeBanking y Banca Comercial.

El motivo de esta selección es clara a partir del último informe publicado por “Anti-Phishing Working Group” (APWG) en www.antiphishing.org.

El ataque a las instituciones financieras representa mas del 90% de este tipo de ataques y es una tendencia que se mantiene. Otra tendencia que se mantiene es el crecimiento de la cantidad de reportes recibidos por parte de la APWG desde su creación, llegando a superar los 15.000 en el mes de Junio.



Resultados Análisis Home Banking

Aunque todos los bancos listados por el Banco Central de la República Argentina en su página Web poseen registrado un dominio sobre el cual ofrecen información sobre la institución, de diversa índole, solamente el 61% de ellos poseen un servicio de Home Banking transaccional para sus clientes⁷ (Ver Gráfico 1).

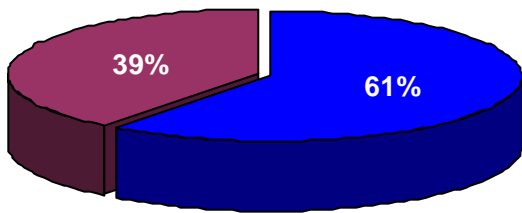


Gráfico 1 - El 61% de los bancos de Argentina ofrecen servicios de Home Banking a sus clientes

El análisis efectuado sobre el universo de instituciones financieras que brindan servicios transaccionales de Home Banking ha permitido detectar que el 16% de los sitios no presentan una o varias de las características de seguridad que han sido consideradas como necesarias en la enumeración anterior (Ver Gráfico 2).

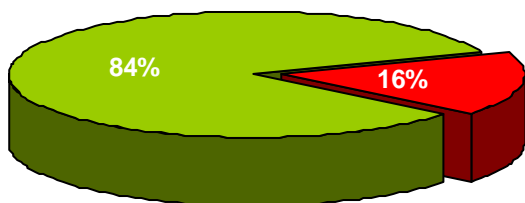


Gráfico 2 - El 16% de los servicios de Home Banking poseen uno o varios errores de diseño que los hacen más vulnerables a un ataque de phishing

Resultados Análisis Banca Electrónica

Los resultados que se han podido obtener en el análisis de los sitios que brindan servicios para empresas son más desfavorables que los

mencionados en el caso de banca personal. También es importante señalar que el número de instituciones financieras que brindan este tipo de servicios es sustancialmente menor: solamente el 30% de los bancos tiene un servicio de esta naturaleza (Ver Gráfico 3).

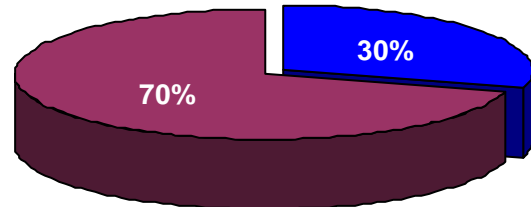


Gráfico 3 - El 30% de los bancos ofrecen servicios de Banca Corporativa a sus clientes

El análisis de los sitios Web que brindan servicios transaccionales de banca para empresas permite concluir que el 29% presenta algún error de diseño que puede ser explotado en un ataque de robo de identidad (Ver Gráfico 4).

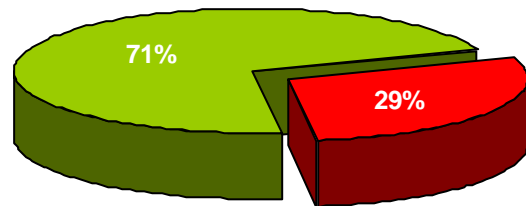


Gráfico 4 - El 29% de los servicios de Banca Corporativa poseen uno o varios errores de diseño que los hacen vulnerables a un ataque de phishing

+ Errores más comunes

Es importante remarcar que el presente informe analiza solamente el diseño de las páginas transaccionales de las entidades financieras de Argentina entendiendo que éste debe generar el mayor nivel de confianza posible para los usuarios y ofrecerle todas las herramientas tecnológicas que se encuentran a su disposición para reducir el riesgo de impersonalización de su sitio Web. No se han analizados otros aspectos tales como: tipo de comunicaciones electrónicas emitidas por los bancos, mecanismo de autenticación empleado, material de capacitación empleado, etc. que son factores que pueden incrementar el riesgo de un ataque de este tipo.

⁷ Los tipos y niveles de servicios ofrecidos por las instituciones financieras se encuentran fuera del alcance del presente informe.



De todos los errores analizados, la falta de visualización del candado es el más común. Esto puede ser debido a que la página utilizada para acceso o para efectuar transacciones posee imágenes (tal como banners) que se encuentran en sitios no seguros o porque se utilizan frames dentro de la página (alguno de ellos no seguros).

Sin embargo, la situación más alarmante es la existencia de sitios que se no poseen instalados certificados digitales, realizando toda la comunicación sobre un canal sin encriptación. Esta omisión genera un riesgo muy alto, tanto para el banco como para aquellos clientes que ingresan sus contraseñas sobre el mismo.

En el gráfico que se muestra a continuación (Gráfico 5) se han resumido los promedios verificados para cada una de las características de seguridad sobre los servicios de Home Banking y Banca Electrónica que se han analizado.

Resulta positivo verificar que la mayoría de los sitios han tenido en cuenta estos aspectos de seguridad al momento de realizar el diseño de los mismos. No obstante, en virtud de la masificación de los ataques de phishing que se está registrando últimamente, resultaría de suma importancia que **todas** las páginas transaccionales de las entidades financieras tuvieran en cuenta las condiciones de seguridad mínimas para brindar este tipo de servicios a sus clientes.

Es importante destacar que el cumplimiento de las condiciones analizadas no supone un gasto considerable para ninguna entidad financiera, máxime si se lo compara con la inversión que supone contar con una aplicación transaccional en línea sobre Internet. En la mayoría de los casos, los problemas pueden resolverse con pequeños cambios de diseño de las páginas involucradas, prácticamente sin costo alguno.

Es importante recordar también, a modo de conclusión, que **los ataques de phishing se fundamentan en el poco conocimiento de los usuarios para poder detectar un mensaje o sitio fraudulento y el bajo nivel de seguridad de los**

mecanismos de autenticación generalmente utilizados⁸.

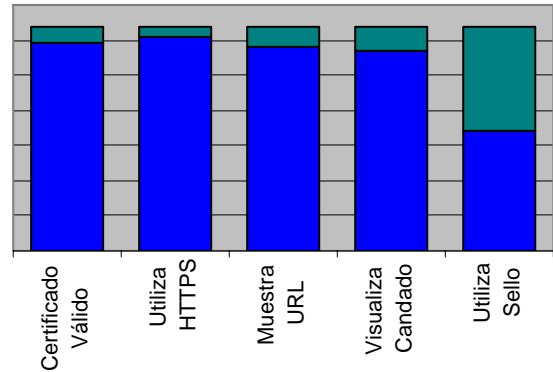


Gráfico 5 – Características de Seguridad incluidas en el Estudio. El extremo superior de cada una de las barras indica el porcentaje de páginas que no cumplen con la condición analizada.

El diseño correcto de los sitios resulta útil cuando el usuario conoce y sabe distinguir estos signos de seguridad descriptos anteriormente. Esta tarea implica una constante capacitación por parte del banco al respecto.

Además, el comportamiento de la institución financiera en las comunicaciones a sus clientes condiciona el nivel de éxito de un eventual ataque de phishing. Por ejemplo, si el usuario recibe habitualmente correos electrónicos de parte del banco, con datos sensibles sin ningún tipo de protección o solicitándole que acceda a un link para obtener o aportar algún tipo de información, es altamente probable que acceda a cumplir con instrucciones contenidas en un correo fraudulento⁹.

Por lo tanto, es sumamente importante que **las entidades financieras instruyan permanentemente a sus clientes** respecto de las tecnologías de seguridad disponibles y las apliquen en sus propios procedimientos en las relaciones electrónicas que entablan con los mismos.

⁸ La tendencia a nivel mundial en esta materia es abandonar los mecanismos de autenticación utilizados hasta ahora por otros basados en dos factores. Ver, por ejemplo, el informe de la FDIC, en: <http://www.fdic.gov/consumers/consumer/idtheftstudy/technology.html>

⁹ Según el informe publicado por “Anti-Phishing Working Group” en www.antiphishing.org, entre el 3% y 5% de los correos electrónicos correspondientes a ataques de phishing tienen éxito.