

Principio 4: “Protege el acceso al Home Banking”

Hoy en día es muy común el uso del Home Banking, brindado por la gran mayoría de los Bancos. Esto se debe principalmente a la cantidad de gente que tiene acceso a Internet y dada la comodidad de consultar en el Home Banking, por ejemplo, el saldo de la tarjeta, la cuenta bancaria o los movimientos y pagos de servicios, todo esto realizado desde el asiento de la casa, el trabajo o un bar.

Esta comodidad a veces puede llevar a que existan riesgos de seguridad y privacidad. Sin embargo, si se tienen los recaudos necesarios, el uso del Home Banking puede ser seguro.

Las medidas de seguridad que se deben utilizar son variadas y depende del contexto en el que se lo use.

El siguiente es un sencillo ejemplo de una situación que puede encontrarse el usuario.

Un usuario utiliza para ingresar a su Home Banking una clave relativamente fuerte (ver *Principio 3: “Usa contraseñas fuertes”*), por ejemplo, una clave de más de 10 caracteres. Esta es una muy buena práctica. Sin embargo, si se ingresa al Home Banking desde la computadora de un cibercafé, la longitud de la clave de acceso al Home Banking puede quedar totalmente insegura ya que la computadora puede tener algún programa que grabe las teclas que presiona el usuario. Incluso puede existir algo más sofisticado, como la captura de pulsaciones del mouse, en caso que el usuario utilice el teclado virtual, que prácticamente todos los bancos hoy en día ofrecen en su página de inicio de sesión en la cuenta bancaria. Por estos motivos, el usuario debe tener presentes las recomendaciones que se presentan a continuación.

Precauciones

Para evitar tener problemas en el Home Banking:

- **Utilizar contraseñas fuertes:** El usuario y contraseña (eventualmente el número de documento) son los únicos medios que protegen al usuario del ingreso indebido a una cuenta bancaria. Por lo tanto hay que colocar una contraseña y/o usuario no deducible por un atacante (ver *Principio 3: “Usa contraseñas fuertes”*).
- **Utilizar una computadora confiable:** No se debe ingresar al Home Banking desde una computadora no confiable. Por ejemplo, una computadora que es utilizada permanentemente por menores, la computadora de un amigo o desde un cibercafé.
- **Utilizar un sistema operativo y programas actualizados:** Es importante tener el Sistema Operativo (Windows o Linux) actualizado y tener instalado y actualizado un antivirus. También es recomendable tener algún firewall activado y todos los programas que se utilicen actualizados a su última versión.
- **No revelar información:** Nuestros datos personales, como nombre, apellido, DNI, usuario y contraseñas; nunca serán solicitados por correo electrónico por el banco. De recibir algún correo de este tipo, ponerse en contacto telefónicamente con el banco para asegurarse que esto sea correcto.



El uso del Home Banking, como ya se dijo anteriormente, es seguro si se toman las medidas preventivas para una operación segura en el mismo.

Autor: Ulises Cuñé - Openware

El presente artículo es uno de los principios publicados por **Openware**, en el marco de la **Semana Internacional de la Seguridad Informática**. Para visualizar el resto de los textos de concientización, consulte el siguiente sitio Web:

http://www.openware.biz/es/noticias/semana_internacional_de_la_seguridad_informatica_principios_de_seguridad_%E2%80%9Cdale_valor_tu_inf

Licencia

El presente artículo es liberado bajo [licencia Creative Commons](#).

Usted es libre de:

copiar, distribuir, exhibir, y ejecutar la obra.
hacer obras derivadas de ella.

Bajo las siguientes condiciones:

- Usted debe atribuir la obra en la forma especificada por el autor o el licenciante.
- Usted no puede usar esta obra con fines comerciales.
- Si usted altera, transforma, o crea sobre esta obra, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.

<http://creativecommons.org/licenses/by-nc-sa/2.5/ar/>