

1.- TU COMPROMISO

Claves

Respondemos tus consultas acerca de la seguridad en bancoedwards.cl, y te recomendamos:

- No ocupes la misma clave del banco para otros sitios en Internet.
- Si tu sistema operativo (Windows u otro) te ofrece “volver a recordar clave”, no lo aceptes nunca.
- No permitas que otros vean tu clave. Pide respeto por tu privacidad.
- Jamás consideres correos electrónicos en donde se solicite tu clave o que pidan cambiarla. Eso nunca lo va a pedir el banco.
- Cambia constantemente tu clave. Cada 2 ó 3 meses es recomendable.
- Nunca des tu clave a terceros. Ni siquiera a funcionarios del banco.
- Crea tu clave con caracteres alfanuméricos no triviales (evita claves como: 123456, abcdef, 111111, aaa111). Claves más difíciles de intuir. Por ejemplo: sw19ee, krte12r, etc...
- Si vas a tener un periodo largo de inactividad con tu clave, es mejor que la bloques por ese tiempo.

bancoedwards.cl

Es un portal seguro, pero ten en cuenta lo siguiente:

- Evita entrar a bancoedwards.cl desde cibercafés u otros locales públicos.
- Mira si la URL de bancoedwards.cl está bien escrita. A veces ocupan “páginas falsas” con direcciones extrañas.
- Entra siempre a bancoedwards.cl desde el navegador.
- Nunca entres al sitio desde correos electrónicos
- Denuncia al teléfono (600)-380-1888 si te ha llegado algún correo electrónico que consideres sospechoso.
- Ocupa navegadores que acepten correctamente la encriptación que ocupan nuestros servidores (128 bits) como son Microsoft Internet Explorer 5 ó superior, o Netscape Navigator 5 ó superior.

Compras por Internet

Nunca olvides estas recomendaciones:

- Si vas a comprar en algún sitio de subastas online, sé desconfiado. Siempre debes chequear la reputación de tu contraparte, para evitar encontrarte con actos ilícitos posteriores.
- Usa un explorador de red seguro: Netscape Navigator y Microsoft Internet Explorer, proporcionan seguridad para una encriptación confiable.
- Busca siempre que la URL de los sitios de compra, comiencen con https:// (en vez de http://) y que tengan la imagen de un candado.
- Guarda una copia de todas tus transacciones. Incluye la copia del registro de transacción y dirección de Internet.
- Puedes utilizar el sistema de contra entrega de Correos de Chile, donde el producto se despacha y al momento de ser entregado se pide el dinero de la compra-venta, de no realizarse el pago no se entrega o viceversa. Visita Netcompra.cl
- Paga siempre usando Pago Seguro del Banco Edwards

Comercio Tradicional

Cuida tu tarjeta y considera estas recomendaciones:

- No pierdas de vista tu tarjeta. Vigila que no le tomen fotos ni la deslicen por otras máquinas.
- En "Últimos movimientos facturados", puedes consultar en línea las compras de tu tarjeta.
- Jamás le entregues la fecha de vencimiento ni el número de tu tarjeta a terceros por teléfono, a menos que tú hayas generado la llamada.
- Evita que impriman dos recibos de tu transacción.
- Firma tus Tarjetas de Crédito nuevas inmediatamente al recibirlas. No dejes los espacios para firmar en blanco, pues ello permite que los ladrones falsifiquen la firma en las tarjetas y recibos de transacción.
- Al recibir el estado de cuenta de tu tarjeta, revísalo contra las copias de tus recibos de transacción para detectar inmediatamente cualquier discrepancia.

- Asegúrate que se emita un sólo recibo de transacción con el número de tu tarjeta de crédito y guarda siempre tu copia.
- Verifica que el monto en la copia del recibo que te haya entregado el comercio (copia del cliente) sea el mismo que aparece en el recibo de transacción (copia del comercio).
- No permitas que los cajeros o vendedores anoten tu dirección o número telefónico en el recibo de transacción, ni el número de tu tarjeta de crédito en los cheques. Esta información no le sirve de nada al vendedor; al contrario, aumenta el riesgo de fraude.
- Nunca firmes un recibo de transacción en blanco. Alguien podría llenarlo con un monto falso.

Call Center

Cuando se contacten contigo, asegúrate lo siguiente:

- Haber escuchado claramente el nombre y apellido de quién llamó, e intentar memorizarlo.
- Si no es tu ejecutivo de Cuentas, sino un operador/a de un Call Center, y te plantea que algo urgente va a ocurrir con tu cuenta, ten cuidado, ya que puede ser una llamada falsa.
- Jamás entregues las claves de tu cuenta en caso de una llamada a tu casa u oficina. En caso contrario, cuando tú eres el que generó la llamada, la persona autorizada te preguntará estos datos, los cuales debes ingresarlos desde las teclas de teléfono, nunca verbalmente.
- Ten claro el nombre de tu ejecutivo de cuenta. Si alguien te llama diciendo que es tu “nuevo ejecutivo”, lo mejor sería que le pidieras el nombre de tu “antiguo ejecutivo”, para verificar que es alguien del Banco. En caso de igualmente sospechar, pide que te llamen en un rato más y aprovechas de contactarte con el Banco para confirmar el nuevo nombre.

Cajeros Automáticos

- Sé discreto en contar tu dinero.
- No permitas que gente que espera su turno, esté muy cerca de ti.

- Cuando estés esperando, también mantén una distancia prudente con el que saca dinero.
- Guarda tu dinero antes de salir a la calle.

2.- NUESTRO COMPROMISO

Claves

La llave personal a tu cuenta debe ser completamente secreta. Por nuestra parte nos comprometemos:

- El proceso de identificación y autenticación (que seas realmente tú quien ingresa al sitio) se desarrolle de manera confiable, a través de bases de datos custodiadas.
- Bloquear las claves si se ingresan erróneamente más de 3 veces.

bancoedwards.cl

Es el portal a las cuentas de nuestros clientes. Ponemos especial atención a la seguridad:

- Para ti que todavía desconfías transferir dinero por Internet, creamos Digipass, un dispositivo generador de claves que asegura que aunque roben tu clave original, sin Digipass, jamás podrán hacer una transferencia por ti.
- Encriptación. La comunicación entre tu equipo y los servidores del banco debe estar libre de cualquier intromisión. Eso se logra encriptando los datos mientras viajan por internet, quedando ilegibles para quien intente leerlos.
- Botón Cerrar. En Banco en Línea puedes cerrar tu sesión con el botón Cerrar. Así, si alguien intenta ocupar tu PC mientras no estés, no podrá acceder a tu cuenta.
- Cerramos tu sesión después de 5 minutos de inactividad. Si mientras realizas tus operaciones, necesitas abandonar tu computadora y no has cerrado tu sesión, por seguridad la cerramos nosotros después de 5 minutos.

- Servidores certificados. Nuestros servidores están certificados por VeriSign, una Autoridad de Certificación líder en el mundo.

Compras por Internet

Para que le pierdas el miedo a comprar por Internet, nuestro compromiso es ofrecerte productos de seguridad:

- PagoSeguro: Es una tarjeta “virtual” que el banco te ofrece cada vez que quieras hacer un pago por la web. Esta tarjeta tiene un número y una fecha de vencimiento único, que expiran una vez que se haya concretado la compra o después de 48 horas. Se puede pedir PagoSeguro las veces que sea necesario.
- Certificados digitales. Ponemos a tu disposición la emisión de Certificados Digitales para la firma electrónica de transacciones, asociadas a Pagos con Nóminas y Transferencias de Fondo a Terceros.

Comercio Tradicional

- El “mundo real” también presenta peligros para los clientes que manejan Tarjetas de Crédito.
- Monitoreamos permanentemente la actividad de las Tarjetas de Crédito para identificar a tiempo posibles fraudes o clonaciones.
- Poseemos procesos rápidos informativos y de bloqueos de tarjetas.

Call Center

Estamos atentos a responder sobre cualquier consulta acerca de tu seguridad en bancoedwards.cl:

- Teléfono dedicado a consultas sobre seguridad. Mesa de Ayuda Internet (600)-3801888

- Información clara y didáctica acerca de los procesos de seguridad que utiliza el Banco.
- Advertencias oportunas sobre fraudes que estén dando vueltas por la red.

Si el Banco requiere comunicarse contigo vía teléfono, nuestro compromiso es:

- Los operadores o ejecutivos se identificarán adecuadamente y te darán la información necesaria para que después puedas confirmar su nombre.
- Ninguno te preguntará acerca de tu clave.
- Si tú generaste la llamada y el ejecutivo para contestarte requiere tus datos personales, al ingresar tu RUT y clave, deberás hacerlo en tu teléfono y jamás darlos verbalmente.

Privacidad

Al tener una cuenta corriente, cada banco maneja datos como nombre, domicilio, correo electrónico, nacionalidad, etc... Nuestro compromiso es administrar esta información de la manera más transparente y adecuada:

- Jamás compartir estos datos con empresas u organizaciones sin tu consentimiento (a excepción que la ley o el gobierno lo requiera)
- Los datos demográficos siempre representan información agregada y nunca identifican a un usuario específico.
- Enviarte información sobre servicios o productos de interés, siempre y cuando nos hayas dado tu autorización.

3.- CÓMO DETECTAR FRAUDE

Mails

Si recibes un mail sospechoso, ten en cuenta lo siguiente:

- Te solicita que hagas click en él, llevándote a una página “muy parecida” a la del Banco.

- Te pide que le des información personal.
- Presenta en muchos casos, errores ortográficos.
- Anuncian cambios en las cuentas, creando una sensación de urgencia.

Compras por Internet

A veces cuesta detectar a inescrupulosos que engañan a través de la web. Mantente atento ante:

- Sitios “nuevos” de e-commerce pueden abrir sospechas. Si al averiguar de dónde proviene, quiénes son sus dueños y toda información es muy confusa, podrías estar frente a una acción ilícita.
- En caso que todo “te suene en regla”, averigua las formas de pago y de entrega que te ofrece. Si es un proceso engorroso, donde sospeches que exista un riesgo elevado para ti, cancela la compra.
- Chequea en Internet la existencia de la empresa en la cual deseas comprar. Si en los buscadores no encuentras nada, información confusa o alegatos de otros usuarios, te recomendamos que no compres, hasta asegurarte.

En el Comercio Tradicional

Mantente atento a las siguientes situaciones cuando pagues con tu tarjeta:

- Si al que le entregaste tu tarjeta, ves que saca un celular en ese mismo momento, podría querer sacarle una foto.
- La máquina donde desliza tu tarjeta no sea las oficiales, o que estén con deterioros sospechosos.
- La boleta aparece con otro monto.
- La boleta aparece sin ningún monto.

Llamadas telefónicas

Llamadas extrañas, que involucren concursos y que mencionen programas de televisión conocidos.

- Personas que se compliquen en contestar preguntas sobre el origen de la llamada o lo hagan muy rápido dándole poca importancia.
- Si te hacen preguntas personales (nombre y apellido, domicilio, fecha de nacimiento, etc...), te piden claves de tarjetas o te piden que compres algo en ese instante.
- Si es celular que te envíen mensajes sospechosos, pidiéndote que les devuelvas la llamada.

4.- QUÉ HACER EN CASO DE FRAUDE

Fraude en el “mundo virtual”

Comunícate inmediatamente con emergencias bancarias del Banco al 600 380 18 88.

- Intenta recordar todos los detalles, haciendo una cronología de qué exactamente fue lo que compraste, los montos, los medios de pago, la URL, etc...
- Informa el fraude a BRICIB Brigada Investigadora del CiberCrimen al 697 48 84.

Fraude en el “mundo real”

- En caso de tener problemas en Chile con tus Tarjetas de Crédito, porque fueron robadas, capturadas por un cajero automático o perdidas accidentalmente, debes bloquearla inmediatamente en Fonobank 600 380 18 88 o a través de emergencias bancarias en bancoedwards.cl
- En el caso que te encuentres en el extranjero y necesites que te bloqueen tu tarjeta, puede comunicarte con los servicios de emergencia de Visa Internacional o MasterCard International.