

¡En MONEX estamos comprometidos con tu seguridad!

Te compartimos algunas sencillas medidas para que puedas navegar en tu Servicio en Línea de manera segura.

Seguridad Servicio en Línea	1
Tus Responsabilidades	1
Riesgos	2
Espionaje	2
Phishing	2
Pharming	2
Smishing	2
Vishing	3
Recomendaciones	3
Contáctanos	3



Seguridad Servicio en Línea

La seguridad en el servicio en línea es un compromiso para Grupo Financiero Monex (MONEX), por lo que toda la comunicación operativa entre tu computadora y el sistema central se realiza en nuestro sitio seguro (https) utilizando alta encriptación de 128 bits, esto significa, que en el remoto caso de que un mensaje sea interceptado, no podrá ser descifrado o modificado. Estas medidas de seguridad, junto con otras que MONEX ha incorporado, garantizan que el medio para el Servicio en Línea por el cual se pueden hacer consultas u operaciones se realicen con máxima eficiencia y confidencialidad.



Tus Responsabilidades

Antes de utilizar los Servicios en Línea de MONEX, debes de leer y comprender los términos y condiciones explicados en tu **contrato de servicio**, en el que se describe en detalle todos los aspectos de uso.

Tus claves de acceso son confidenciales, por ningún motivo las proporcionas a terceros. Te recomendamos memorizarlas y no anotarlas, ni conservarlas en archivos de tu computadora. Tú eres responsable de mantener confidencial la contraseña, números de contrato, información personal de identificación y otros datos de tus contratos.

MONEX no se hace responsable de errores del cliente o negligencia al usar los Servicios en Línea y no cubre pérdidas ocasionadas por:

- ✘ Errores de captura o el uso indebido del servicio.
- ✘ Negligencia en el manejo o compartir la contraseña que ocasione accesos de personas no autorizadas a tu Servicio en Línea.
- ✘ Dejar la computadora sin atención durante una sesión en línea.
- ✘ Injustificados retrasos en el reporte de incidentes de accesos de personas no autorizadas a las sesiones en línea del cliente.





Riesgos

Existe el riesgo de que personas deshonestas se hagan pasar por ti con fines fraudulentos y puedan acceder a tu Servicio en Línea para sustraer tus fondos. Es común encontrar que un fraude sea cometido por alguien cercano a nosotros, como familiares, amigos o colaboradores en la empresa. Utilizar contraseñas fácilmente predecibles aumenta el riesgo de que alguien las deduzca.



Espionaje-Puede haber alguien vigilándote cuando ingreses a tus servicios de Banca en Línea. Cuando entres a tu servicio, ten cuidado de no ser observado.

¿Qué se recomienda? No utilices sitios públicos como cafés Internet, centros de negocio en hoteles o aeropuertos para entrar a tu Banca en Línea, si lo haces, cambia tus contraseñas lo más pronto posible en una máquina segura.



Phishing-Es un delito del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común a través de un correo electrónico, o algún sistema de mensajería instantánea o incluso, realizando también, llamadas telefónicas.

¿Qué se recomienda? Elimínalo y no proporciones la información que te solicitan. En caso de que hayas completado las instrucciones de llenado, te pedimos cambiar tus claves de inmediato y llamar a nuestro Centro de Atención.



Pharming-Es la explotación de una vulnerabilidad en los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario accederá en su explorador de Internet a una página falsa, la cual el atacante haya especificado para ese nombre de dominio.

La infección del equipo se lleva a cabo por la ejecución de archivos "dudosos" recibidos por correo o al ingresar a ligas de páginas aparentemente de "interés" o noticias escandalosas.

¿Qué se recomienda? Nunca abras o ejecutes archivos con información que no esperabas recibir, aun cuando el título del mensaje parezca normal. No ingreses a ligas de páginas recibidas por correo o Messenger, ya que desde el primer click se puede iniciar la infección de tu equipo.



Smishing-Es un nuevo tipo de delito o actividad criminal usando técnicas de ingeniería social, empleando mensajes de texto dirigidos a los usuarios de Telefonía móvil. Las víctimas de Smishing reciben mensajes SMS con líneas similares a estas: "Estamos confirmando que se ha dado de alta para un servicio de citas. Se le cobrará 2 dólares al día a menos que cancele su petición: www.?????.com." Cuando visitamos la dirección web, las víctimas son incitadas o incluso forzados a descargar algún programa que en su mayoría suele ser un Troyano.

¿Qué se recomienda? No ingreses a ligas de páginas recibidas por teléfono, frente a alguna duda, lo más conveniente es llamar a nuestro Centro de Atención para preguntar si hay algún problema en la cuenta.





Vishing- Es un delito donde se utilizan grabaciones y la ingeniería social para engañar a personas y obtener información financiera para el robo de identidad. El defraudador utiliza un marcador automático para llamar, cuando la llamada es contestada, la grabación se activa y alerta al "consumidor" que están entrando a su cuenta de forma fraudulenta y que debe llamar de inmediato al número que le indican.

¿Qué se recomienda? No proporcionar información confidencial, a no ser que tú te hayas comunicado directamente con la institución financiera.

<http://www> Recomendaciones

► Recomendaciones sobre el uso del Servicio en Línea

En Internet, como en cualquier otro medio, existen riesgos, por lo que te recomendamos que:

- No compartas tus contraseñas de acceso.
- No utilices para tus contraseñas fechas, nombres o lugares que alguien pueda conocer o que se encuentren en documentos de fácil acceso público.
- Para recordar contraseñas complejas, puedes utilizar ciertas letras de alguna frase que conozcas bien, de esta manera tus contraseñas no tendrán sentido para otros y te serán fáciles de recordar.
- No escribas tus contraseñas en papeles y mucho menos las dejes junto a tu máquina o en archivos.
- Resguarda en un lugar seguro tus dispositivos de Acceso.
- Cuando entres al Servicio en Línea, ten cuidado de no ser observado por alguien.

► Recomendaciones sobre notificaciones recibidas por Correo Electrónico

Cuando nos ponemos en contacto contigo por correo electrónico, siempre encontrarás las siguientes características en nuestros comunicados:

- Nuestros correos van siempre personalizados, tu nombre o razón social aparece al principio de los mismos.
- El tema de nuestros mensajes tiene que ver con productos y servicios que MONEX te ofrece, o bien con transacciones que puedes hacer a través de tu Servicio en Línea.



Recuerda que MONEX nunca te pide información sensible como números de cuenta y claves de acceso de ningún medio y nuestros correos son siempre personalizados. Si recibes cualquier correo electrónico de Monex que no tenga las características que te hemos mencionado, por favor, denúncialo al llamar al Centro de Atención.

► Recomendaciones de Protección

Como principal defensa para tu equipo de cómputo, existen los antivirus contra los ataques y amenazas de delincuentes cibernéticos (hackers, crackers). La mayoría de los antivirus se actualizan en línea de forma inmediata al encender la computadora.

Sería ideal que adicionalmente al antivirus añadieras programas que detecten la intervención de la computadora por un delincuente, como firewall (cortafuegos), anti-spyware (espionaje en línea), anti-spam (detiene correos masivos no deseados), anti-keylogger (impide la divulgación de datos que un keylogger roba de las entradas del teclado) y anti-troyanos (detiene programas de auto instalación y virus nocivos para el equipo).

► Sitio de interés

Te recomendamos acceder al Portal Seguridad en Internet <http://www.eseguridad.gob.mx/>, donde podrás encontrar información actualizada sobre seguridad.



Contáctanos

Llama al Centro de Atención al **52314500** en el DF ó al **01 800 74 66639**, desde el interior de la República.

