peoplepass

Recomendaciones de seguridad

1. Recomendaciones de uso de portales web

Los delincuentes suplantan páginas web de servicios públicos, telefonía, impuestos, seguros, mensajería, aerolíneas, billeteras virtuales, entre otras páginas; para evitar este tipo de suplantación, ten en cuenta las siguientes recomendaciones:

- No uses buscadores de internet para realizar pagos en línea.
- Cuando realices transacciones, escribe la dirección web oficial.
- No uses sitios web no seguros para realizar pagos.
- Verifica siempre la dirección del sitio web, en caso de ver inconsistencias, no ingreses.
- No realices operaciones bancarias desde dispositivos que no sean propios.
- Al realizar cualquier tipo de transacción asegúrate de activar el código CVV2 dentro de nuestra APP.

01.

2. Recomendaciones de uso de la APP

Ten en cuenta las siguientes recomendaciones para el uso de nuestra APP:

- Descarga la aplicación desde los sitios oficiales.
- Mantén activa las actualizaciones de la aplicación con la última versión.
- Realiza el registro de la biometría del dispositivo móvil.
- Activa las notificaciones de operaciones en el correo electrónico y por mensaje de texto.
- Configura el bloqueo del dispositivo móvil en el menor tiempo posible y con contraseñas de difícil deducción.
- Evita hacer conexión a redes de WiFi públicas.
- Evita tener activo las opciones de comunicación inalámbrica como NFC (Android) y el Airdrop (IOS).

02.

- Utiliza la aplicación únicamente para los fines y servicios establecidos en el contrato y en los términos y condiciones.

- Asegúrate de gestionar tus productos dentro de la app móvil y siguiendo los parámetros de seguridad como la activación del CVV2 para tus transacciones; este código no se debe compartir con terceros.

3. Crea tu clave y contraseña de forma segura

Tus claves y contraseñas deben ser creadas de forma segura; estas deben ser fáciles de recordar y difíciles de adivinar:

- Por ningún motivo se deben compartir los usuarios y contraseñas.
- Debemos realizar cambios periódicos de contraseñas.
- Evitemos el uso de nombres, fecha de nacimiento o cualquier otro criterio personal evidente.
- Crea contraseñas seguras y utiliza una diferente para cada aplicación y entorno.
- En caso de que tengas dudas sobre un posible hackeo, cambia de contraseña, solicita la reexpedición de tu tarjeta y repórtalo de forma inmediata a la línea de atención de Servicio al Cliente.

03.

4. Evita que realicen compras con tu celular

Evita que realicen compras con tu celular teniendo en cuenta estas recomendaciones:

- Desactiva el NFC (Android) y el Airdrop (IOS) cuando no lo estés usando.
- Configura el bloqueo de la pantalla en el dispositivo con un método robusto (biometría facial, huella digital o una contraseña de difícil deducción).
- Presta atención a los avisos de compras recibidas en tu celular o correo electrónico.
- Mantén tu celular actualizado con la última versión del sistema operativo y sus aplicaciones.
- Configura la pantalla para que se apague en el menor tiempo posible.
- Mantén vigilado tu celular en lugares públicos.
- Evita prestar tu celular a desconocidos.

04.

5. Recomendaciones para hacer compras más seguras en Internet

Realiza compras online de forma segura con las siguientes recomendaciones:

- Compra en sitios seguros y oficiales. Para saber si una página es confiable, la dirección web debe contar con el prefijo https (y mostrar al lado el ícono del candado) con un certificado digital válido.
- Evita los enlaces de correos electrónicos y anuncios.
- Ten cuidado en las redes sociales, puedes encontrar páginas falsas, anuncios fraudulentos o enlaces maliciosos en los comentarios.
- No almacenes tus datos de pago.
- Desconfía de los precios excesivamente bajos.
- Realiza tus compras online desde un dispositivo con antivirus actualizado, para evitar recibir programas que puedan robar tu información.
- Evita conectarte desde redes WiFi públicas.
- Apaga las compras por internet en las tarjetas y solo activa esta opción cuando realmente vayas a hacer uso de la tarjeta para una compra por internet.
- Una vez realices una compra por internet, debes estar atento a responder una llamada de un número desconocido, porque puede ser desde nuestra área de Monitoreo Transaccional queriendo confirmar la transacción; en ningún momento nuestra área de Monitoreo y/o Servicio al Cliente te pedirán datos como contraseñas, CVV o código de seguridad de la tarjeta.
- En caso de inscribir tus datos de pago en sitios no oficiales o autorizados, PeoplePass no se hace responsable de las compras online que resulten fraudulentas.

05.

6. Recomendaciones para evitar que clonen tu tarjeta en cajeros automáticos

Evita que clonen tu tarjeta con las siguientes recomendaciones:

- Verifica que el cajero automático no tenga anormalidades.
- Por ningún motivo compartas tu clave y recuerda cambiarla con frecuencia.
- Al ingresar tu clave, cubre el teclado con tu mano.

06.

- No aceptes ayuda de terceros por ningún motivo.
- Guarda tu tarjeta antes de abandonar el cajero.

En caso de pérdida o robo de la tarjeta, debes llamar a la línea de Servicio al Cliente para bloquearla o también puedes realizar esta acción desde la APP.

7. Recomendaciones para prevenir los fraudes telefónicos

Las llamadas de desconocidos pueden ser intentos de fraude. Te damos algunas recomendaciones para tener en cuenta:

- No accedas a uso de cajeros automáticos si estás siendo guiado por teléfono.
- No hagas transferencias de dinero luego de recibir una llamada sospechosa.
- No generes claves ni brindes datos confidenciales en ninguna llamada.
- Cuelga de inmediato si desconfías de la llamada.
- Llama a nuestra línea de Servicio al Cliente si presentas dudas de algún movimiento. En PeoplePass nunca te llamaremos para pedirte datos confidenciales.

07.

8. Mantén tu seguridad también en redes sociales

La información que compartes en redes sociales puede ser usada contra ti. Te damos algunas recomendaciones para proteger tu identidad digital:

- Evita publicar información bancaria o de tus compras.
- Cuida con quien compartes tus publicaciones.
- Configura correctamente los ajustes de privacidad de tus redes sociales
- Activa el doble factor de autenticación en los servicios que lo permitan.
- Comprueba cada cierto tiempo qué información tuya existe publicada en Internet.
- Borra tus datos de navegación de forma periódica (cookies, caché, historial).
- Desactiva la geolocalización si no la necesitas.

08.