RECOMENDACIONES DE SEGURIDAD
Prevención de fraude, suplantación y Seguridad de la Información
¡Piensa antes de actuar!

Recomendaciones de uso del portal 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:

- Protege tus datos personales, ellos son valiosos.
- No uses buscadores de Internet para realizar pagos en línea.
- Utiliza antivirus y otras herramientas de seguridad con actualización automática.
- Actualiza tu sistema operativo, tu navegador y conoce los recursos de seguridad de cada uno de ellos.
- 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.
- Tus contraseñas deben ser seguras, complejas y muy difíciles de adivinar.
- Mantén backups de la información que consideres importante.
- Si no vas a utilizar tu computadora por mucho tiempo, desconéctala de Internet; cuando está desconectada, la computadora no envía ni recibe información de la red y no está vulnerable a hackers o cualquier otro tipo de riesgos surgidos de Internet.

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.
- Actualiza constantemente tus contraseñas.
- Evita tener activa las opciones de comunicación inalámbrica como NFC (Android) y el Airdrop (IOS).
- 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 generación del CVV2 dinámico para tus transacciones; este código no se debe compartir con terceros.

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.
- Evita recibir ayuda de un desconocido. Si necesitas apoyo para realizar alguna transacción en el cajero, acude a un funcionario de la sucursal bancaria.
- Evita que algún tercero vea el número, fecha de vencimiento, nombre y código de seguridad de tu tarjeta.
- Guarda tu tarjeta antes de abandonar el cajero.
- Nunca des los datos de tu tarjeta a nadie, ya sea por correo electrónico, teléfono, WhatsApp, redes sociales o SMS. No entregues tu tarjeta a otra persona. Recuerda que la tarjeta es de uso personal. Verifica constantemente la recepción de las alertas de seguridad o alertas transaccionales.
- En caso de pérdida o robo de la tarjeta, debes llamar inmediatamente a la línea de Servicio al Cliente para bloquearla o también puedes realizar esta acción desde la APP.

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.

Evita que realicen compras con tu celular

Evita que realicen compras con tu celular con 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.

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.
- 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.
- Evita compartir información en sitios dudosos.

En caso de inscribir tus datos de pago en sitios no oficiales o autorizados, PayCash no se hace responsable de las compras online que resulten fraudulentas.

Recomendaciones para prevenir los fraudes telefónicos

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

- Haz tus llamadas desde lugares seguros, donde personas no oigan lo que estás hablando o vean tu contraseña al marcarla en el teléfono.
- No utilices dispositivos de otras personas, porque tus datos pueden quedar almacenados en la memoria del celular.
- 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.
- Los colaboradores de PayCash no están autorizados a pedir tu contraseña. No la informes bajo ninguna circunstancia.
- Llama a nuestra línea de Servicio al Cliente si presentas dudas de algún movimiento.
- PayCash nunca llama a los clientes solicitando datos personales, contraseñas, ni otros datos confidenciales.
- En caso de duda, entra directamente en contacto con PayCash por los canales oficiales de la línea de Servicio al Cliente.

Protege tu identidad digital

- No compartas tus datos personales (número de cédula, claves, códigos SMS o token) por teléfono, redes sociales o mensajes; PayCash no solicita este tipo de información.
- Evita usar redes Wi-Fi públicas para acceder a la App y/o al portal web. Evita acceder a tus cuentas desde equipos públicos o compartidos, estos dispositivos pueden tener software malicioso o configuraciones inseguras que ponen en riesgo tu información.
- Cambia tus contraseñas regularmente y asegúrate de usar combinaciones largas que contengan letras, números y símbolos.
- Evita guardar contraseñas en los navegadores; esta práctica puede ser riesgosa si otras personas tienen acceso a tu dispositivo o si este se ve comprometido.
- Utiliza mecanismos de protección ofrecidos por PayCash, activa alertas y notificaciones y utiliza claves dinámicas.
- No permitas a terceros hacer uso de la funcionalidad, ni facilitarles información que ponga en riesgo tus datos de acceso a la App PayCash.

Debes estar atento a señales de suplantación o fraude

- Haz caso omiso a mensajes sospechosos que prometen premios, bonos, subsidios o falsas promociones en donde te solicitan datos personales o información de tus productos en PayCash.
- Sé muy cuidadoso con los correos o llamadas que aparentan ser de PayCash, verifica que estas comunicaciones no tengan errores ortográficos, URL extrañas o te soliciten datos sensibles como contraseñas y/o datos de la tarjeta.
- Evita abrir o descargar archivos adjuntos de correos electrónicos no solicitados o de remitentes desconocidos.
- Revisa periódicamente tus movimientos o transferencias, con el fin de asegurarte que no existen transacciones no reconocidas en tu depósito.
- No permitas que personas desconocidas te asistan en cajeros automáticos.
- Desconfía si te piden una foto de tu cédula o tarjeta; ninguna tienda legítima solicita escaneos, fotos o archivos adjuntos de tus documentos para procesar una compra. Si los compartes podrías permitir suplantaciones o fraudes financieros.

- No guardes tu tarjeta en sitios que no conoces, algunos sitios ofrecen la opción de "recordar tarjeta", pero no lo hagas si no es una plataforma reconocida.

Utiliza solo canales oficiales

- Descarga la aplicación móvil o accede al sitio web solo desde fuentes oficiales (Google Play, App Store, página web institucional).
- Comunícate siempre a través de los canales autorizados de atención que PayCash ofrece (WhatsApp verificado, línea de atención, redes sociales oficiales).
- Mantén actualizado el software de los dispositivos utilizados y mantén actualizada la última versión de la App PayCash.
- Solo introduce tus datos bancarios en pasarelas de pago seguras como PSE, PayU, MercadoPago o la página oficial de PayCash.

Reporta cualquier irregularidad

- Si sospechas que haz sido víctima de suplantación o fraude, repórtalo de inmediato al canal dispuesto por PayCash para Servicio al Cliente.
- Puedes también denunciar ante:
  Superintendencia Financiera de Colombia (SFC): www.superfinanciera.gov.co
  Policía Nacional – CAI Virtual: https://caivirtual.policia.gov.co
  Fiscalía General de la Nación: Línea 122

Edúcate sobre ciberseguridad

- PayCash realiza campañas de educación financiera y prevención de fraude. Participa y mantente informado.
- Consulta recursos oficiales como:
  https://www.superfinanciera.gov.co/ https://www.sic.gov.co/

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.

Recomendaciones adicionales

- Habilita notificaciones de movimientos en tu App PayCash.
- En caso de que cambies tu número celular o correo, actualízalo en tu perfil de usuario.
- Eres responsable de las transacciones realizadas mediante los mecanismos de autenticación. Por ello, es fundamental que verifiques cuidadosamente la información de cada operación antes de ejecutarla, a fin de evitar errores. Esta responsabilidad se mantiene, salvo que se demuestre una falla atribuible a nuestra entidad.
- Ten en cuenta que no somos responsables de la disponibilidad ni la confiabilidad de tu equipo o de los medios de comunicación que utilices.