Tips de seguridad

Compartamos Banco®

Claves de acceso

Las claves de acceso son las llaves para acceder a tu información son únicas e intransferibles, crea una clave fuerte y segura tomando en cuenta:

- Longitud mínima de 8 caracteres
- Utiliza letras MAYUSCULAS
- Utiliza una letra minúscula
- Utiliza signos como!"#$%&/()=?¡¿'+´,
- No utilices algo que sea común para ti y fácil de descifrar.
- No utilices una contraseña más de una vez
- Realiza el cambio de contraseña mínimo cada 3 meses
- No compartas con nadie tus claves, son totalmente confidenciales
- No escribas tus claves de acceso, la mejor opción es memorizarlas

Descarga app

Descarga tu APP de Compartamos Móvil, solo desde las tiendas oficiales como Google Play o App Store

No. de cliente

Es confidencial y no puedes compartirlo con nadie

Redes WiFi

Evita conectarte a una red WIFI gratuita en centros comerciales, cafés, aeropuertos, etc., para realizar operaciones, estas redes no cuentan con los controles básicos de seguridad, lo cual pone en riesgo tu información personal y financiera.

Actualización y antivirus

Mantén actualizado tu antivirus en tus dispositivos móviles (computadora, tablet, celulares, etc.), al igual que el sistema operativo y el navegador que más utilices.

Correos fraudalentos phishing

Los correos "Phishing" cada vez son más habituales, consisten en enviar correos electrónicos, WhatsApp, mensajes en redes sociales o SMS de forma masiva, suplantando a una entidad (en este caso, bancaria), incluyen un enlace fraudulento cuyo objetivo es dirigir al usuario a un sitio web falso y, así, robar sus credenciales y datos personales. Entre los datos personales del cliente destacan: los nombres de usuario, numero de cliente, números de tarjeta y claves de acceso.

No abras un correo donde te solicite cambiar tus claves de acceso de forma urgente que no hayas solicitado, o donde te ofrezcan un premio, contengan un "link" o enlace que te dirija a otra página donde te pueda solicitar información confidencial o descargar archivos maliciosos "malware".

Enlaces sospechosos

Un enlace sospechoso es aquel que, aparentemente, es fiable, pero cuando das clic al link te redirige a una página falsa que parece ser real o que incluye malware, solocitandote tus claves de acceso.

Robo y suplantación de identidad

Cuida la información que subes a las redes sociales, el robo de identidad y suplantación va en aumento.

El robo de información como datos personales y claves de acceso hacen que los ciberdelincuentes puedan suplantar tu identidad y con esto solicitar o realizar a tu nombre, compras online, créditos bancarios, automotriz o de hipoteca, ubicar donde te encuentras y que sitios recientemente has visitado de acuerdo con tus publicaciones en redes sociales.

La suplantación de identidad consiste en hacerse pasar por alguien, de manera física o digital. De forma física se requiere disponer de documentación real (o falsa) de la víctima a suplantar, de forma digital, simplemente será necesario conocer tu nombre y disponer de alguna imagen que te caracterice.

Valida que información subes y con quien la compartes, realiza la pregunta, ¿es necesario compartirlo?

Alertamiento de movimientos

Solicita tener activo el servicio de alertamiento para que estes enterado de los movimientos realizados en tus cuentas bancarias, por correo electrónico o SMS, en caso de identificar alguno que no hayas realizado, ponte en contacto con su banco.
En Compartamos contamos con un servicio de alertas es sin ningún costo y te permite estar informado de los movimientos de tus cuentas.

Recuerda que en Compartamos, nunca te solicitaremos información personal o claves de acceso por correo o teléfono.