SAN JOSÉ
COOPERATIVA DE AHORRO Y CRÉDITO

DIEZ CONSEJOS DE SEGURIDAD PARA USAR LA COOPERATIVA DIGITAL

El auge de la banca digital también ha traído consigo un aumento de la ciberdelincuencia, que busca aprovecharse de pequeños fallos tecnológicos. Por eso conviene tener en cuenta estas sencillas recomendaciones para sacar el máximo provecho a los servicios bancarios digitales.

SAN JOSÉ
COOPERATIVA DE AHORRO Y CRÉDITO

Por regla general, se debe proteger cualquier dato personal como nombre y apellido, dirección, número de teléfono, correo electrónico, cuenta bancaria y números de tarjetas de débito o crédito. Además sigue y comparte estas recomendaciones:

1. No comparta con nadie las contraseñas de acceso a la banca móvil, ni el código o patrón de acceso a los dispositivos sean estos celulares, tablets o computadoras.

2. Configurar la opción de bloqueo automático en los dispositivos móviles. Se puede hacer mediante el PIN, patrón de desbloqueo, huella digital o si el móvil dispone de la herramienta de reconocimiento facial, aún mejor.

3. No introduzca datos privados en redes 'wifi' públicas puesto que algunas de estas redes abiertas se pueden utilizar para espiar todo el tráfico de datos. De esa forma, se capturan usuarios, contraseñas y otras informaciones para luego hacer un uso fraudulento de las mismas. Para estar seguros, algunas redes 'wifi' solicitan una contraseña. Las que no lo hacen son las denominadas 'redes abiertas'.

4. No guarde contraseñas en celulares, computadoras y no deje almacenados números de cuenta bancarias o números de tarjetas de débito o crédito puesto que son datos confidenciales. En caso que los dispositivos sean robados, el delincuente obtendrá información sensible de los equipos personales.

5. No dé información personal o financiera a través de llamadas, mensajes o correos electrónicos, bajo ningún concepto.

6. Evite las páginas web donde proliferan los enlaces maliciosos como las URL acortadas, los SPAM y la publicidad en ventanas emergentes.

SAN JOSÉ
COOPERATIVA DE AHORRO Y CRÉDITO

7. Se recomienda la descarga de aplicaciones que aumenten la seguridad de los dispositivos como antivirus y aplicaciones que realicen copias de seguridad.

8. Cuando haga operaciones en la página web de la Cooperativa, verifique siempre que la barra de dirección del navegador comienza con 'https' y que muestra un candado. Eso le permite saber que tiene una conexión segura antes de ingresar cualquier tipo de información personal (https://enlinea.coopsanjose.fin.ec/).

9. Evite tener la misma contraseña en aplicaciones como el correo electrónico o redes sociales como Facebook, Twitter y Youtube. Quizás no sea alarmante si se 'hackea' una cuenta social pero ¿qué sucederá si el ciberdelincuente prueba esa información para ingresar a su cuenta de la Cooperativa?

10. Esté al tanto de las informaciones oficiales de la Cooperativa. Si se recibe un e-mail que parezca sospechoso, no haga 'clic' para no caer en una trampa de 'phishing'. Este es un método muy utilizado por los ciberdelincuentes para que la víctima revele sus contraseñas o datos de tarjetas de crédito y cuentas bancarias. Lo hacen mediante correos electrónicos fraudulentos que los redirigen a un sitio web falso donde solicitan información sensible.

Compartir esta información importante con amigos y familiares, para juntos evitar caer en cualquier tipo de estafa bancaria.