Banco Cooperativo Coopcentral

Recomendaciones de seguridad al momento de realizar transacciones por los canales digitales

- Mantener actualizado el sistema operativo y de seguridad de los equipos en los cuales realizan operaciones transaccionales con recursos públicos; como también la actualización periódica del software de antivirus instalado en los equipos.
- No compartir las credenciales (usuario/contraseña) – tokens los cuales son de carácter personal e intransferible.
- Establecer controles efectivos para la custodia de los elementos de seguridad como los tokens – para mantenerlos resguardados en cajas de seguridad (cajas fuertes) con acceso únicamente para el personal autorizado para tal fin.
- No compartir con otros usuarios los equipos desde los cuales se realizan operaciones transaccionales, los cuales deben ser de uso exclusivo de los administradores de las cuentas
- No ingresar a los portales transaccionales desde otros equipos diferentes a los establecidos por la Entidad para el desarrollo de estas actividades.
- No guardar contraseñas en computadoras. Tampoco almacenar números de cuenta bancarias o números de tarjetas de débito o crédito puesto que son datos confidenciales.
- Verificar siempre la dirección web (URL) a la que ingresa – así mismo verificar siempre que la barra de dirección del navegador comienza con https:// y que muestra el candado.
- Digitar la dirección de la página web a ingresar, así mismo evitar el emplear enlaces (links) en correos electrónicos, SMS, mensajes de WhatsApp, banners – los cuales pueden conducirlo a páginas web falsas y/o de suplantación.
- Evitar las páginas web donde proliferan los enlaces maliciosos como las URL acortadas, los Spam y la publicidad en ventanas emergentes.
- Atender oportunamente los mensajes de texto o correos electrónicos que se envían notificando las operaciones realizadas, aun cuando ellos se reciban en horarios no hábiles.
- Verificar con frecuencia el saldo de las cuentas – validando transacciones, movimientos realizados.
- No abrir correos de dudosa procedencia, no instalar archivos que puedan contener software malicioso ni navegar por sitios desconocidos en los equipos donde se realizan las operaciones.
- Inscribir un correo institucional para la notificación de las operaciones transaccionales realizadas.
- Estar al tanto de las informaciones oficiales del Banco – por ejm. si se recibe un e-mail que parezca sospechoso, no hacer '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 lo redirigen a un sitio web falso donde solicitan información sensible.
- Implementar estándares de seguridad, calidad e idoneidad, para la contratación de terceros encargados de la revisión y mantenimiento de los equipos e instalación de software o hardware que soportan la realización de operaciones.
- Implementar mejores prácticas y metodologías de Seguridad de la Información y Ciberseguridad.

Dentro de nuestro portal web encontrara más recomendaciones de seguridad: https://www.coopcentral.com.co/apps_web/portal/seguridad.html