Ciberdelincuencia: Tips para proteger tu dinero

Con la digitalización de la economía y los aplicativos de los bancos en los teléfonos celulares, la ciberdelincuencia está a la orden del día, por ello hay que tener mucho cuidado en las transacciones en línea.

Los ciberdelincuentes utilizan diferentes técnicas, pero principalmente las conocidas como **ingeniería social,** en donde buscan engañarnos mediante mensajes, llamadas telefónicas o comunicaciones supuestamente oficiales por parte de los bancos para que brindemos nuestra información personal y/o financiera.

Tips contra ciberdelincuencia

Por ello, **el subgerente de Prevención del Fraude de BanBif, Aldo Díaz,** brindó las siguientes recomendaciones para proteger nuestra cuenta de ahorros bancaria y de la ciberdelincuancia.

1. Considera contratar un seguro de protección de tarjetas.
2. Activa las notificaciones de operaciones para recibir un correo y SMS luego de cada transacción.
3. No hagas uso de redes wifi públicas.
4. Mantén tu celular actualizado.
5. Descarga la aplicación del banco (app) desde las tiendas oficiales dependiendo de tu móvil.
6. Utiliza una contraseña robusta y cámbiala regularmente.
7. Ante algún robo o pérdida del celular es importante

llamar lo más pronto posible a la banca telefónica para bloquear tu banca digital y desafiliarte del token digital en caso lo veas necesario.

Phishing

Asimismo, Díaz explicó que el phishing, vishing y smishing son algunos de los fraudes electrónicos que utilizan mayormente los ciberdelicuentes para robar datos privados.

En el caso del **phishing** es una técnica de ingeniería social en donde el ciberdelincuente haciendo uso de correos o mensajes busca engañar al usuario para acceder a sitios falsos que tienen un look&feel parecido a la página oficial y en donde brindemos nuestra información personal y financiera para cometer fraude.

En ese sentido**, aseveró que para evitar ser víctima del phishing se debe tener en cuenta que el banco jamás te solicitará tus datos personales por ningún medio: llamada, SMS, correo, WhatsApp.** Asimismo aconseja desconfiar de los mensajes donde se te solicite datos financieros.

El vishing y smishing son variantes del phishing, en donde la principal característica es la modalidad que usa para comunicarse con el cliente, siendo voz (audios, llamadas) y mensajes (SMS, WhatsApp), respectivamente.

Además refiere a que actualmente, diversas entidades bancarias siguen utilizando los SMS para enviar comunicaciones y códigos

de verificación (token SMS), los ciberdelincuentes envían SMS simulando ser alguna notificación oficial, conteniendo un link dentro del mensaje (para ingresar desde el navegador del celular), haciendo que este tipo de técnicas sea muy utilizado por los ciberdelincuentes por su facilidad en la ejecución.

Llamada sospechosa

Por último, Díaz señaló los pasos a seguir en caso de haber recibido una llamada sospechosa en donde haya brindado información personal, son los siguientes:

1. Comunicarse inmediatamente con el banco para bloquear sus tarjetas de débito y/o crédito.
2. Solicitar el bloqueo de su banca digital.
3. Solicitar la desafiliación de su token digital.
4. Con una nueva tarjeta restablecida, proceder con el cambio de sus contraseñas.