Descubre cómo los ciberdelincuentes se pueden hacer pasar por tu banco

- ***Los ciberdelincuentes utilizan técnicas como el vishing (llamadas fraudulentas) para engañar a los clientes y solicitar información confidencial***

- ***En situaciones de seguridad, la entidad puede comunicarse con el cliente para verificar transacciones y proteger la cuenta contra fraudes***

31 de mayo de 2024

Es crucial **ser cauteloso a la hora de recibir llamadas de números desconocidos, ya que pueden ser intentos de fraude**. Sin embargo, es cierto que en ocasiones las entidades contactan con sus clientes por distintas razones, como avisar al cliente que tiene una tarjeta solicitada, pendiente de recoger en la oficina, entre otras.

Otra razón, podría ser para verificar si se realizan gestiones desde la banca *online*, confirmar por seguridad las operaciones. O bien, citar al cliente en una entrevista presencial en la oficina *retail*.

Estas **son algunas de las situaciones más comunes**, en las que **la entidad puede contactar con sus clientes, para proporcionarles información relevante o verificar la autenticidad de las transacciones,** por motivos de seguridad. A pesar de ello, siempre se debe mantener precaución y verificar la legitimidad de las llamadas que se reciben.

¿Es posible que alguien se haga pasar por un empleado del banco y te llame?

Las llamadas fraudulentas (conocidas como *vishing*), son una realidad cada vez más común en la era digital. Los ciberdelincuentes están continuamente mejorando sus técnicas para engañar a sus víctimas.

Los ciberdelincuentes están constantemente perfeccionando sus técnicas para engañar a los clientes. Entre las más utilizadas están, un amplio y profundo **conocimiento de la banca *online***, permitiéndoles guiar al cliente a través de los procesos de gestión para obtener información personal. La **suplantación de identidad** es otra técnica que utilizan para manipular el identificador de llamadas para hacer creer a la víctima que la llamada proviene del número oficial de la entidad. Y el **uso de argumentos convincentes** para ganarse la confianza de los clientes y ofrecer ayuda para resolver problemas falsos de sus cuentas.

Es fundamental recordar que, aunque la llamada parezca legítima, **nunca se deben proporcionar datos personales por teléfono**, a menos que el cliente esté seguro a quien le está proporcionando la información.

Las estafas más recurrentes entre los ciberdelincuentes son las siguientes:

Solicitar **datos confidenciales** como el número de tarjeta o claves de acceso a la banca online, o bien instar a realizar un pago bajo la premisa de una supuesta devolución de dinero.

Es habitual que **utilicen sistemas de pago inmediatos** como BIZUM o soliciten la **retirada de dinero efectivo de un cajero automático** mediante un código personal. CaixaBank permite retirar dinero a través de un cajero automático, mediante un código personal, que ofrece grandes ventajas de seguridad, pero puede llegar a suponer un pretexto común para los ciberdelincuentes a la hora de realizar este tipo de estafas.

Un pretexto común suele ser es que alguien está realizando un reintegro en un cajero automático y que, para cancelarlo, debe seguir los pasos indicados por los estafadores, quienes guiarán al cliente para completar el retiro de dinero efectivo.

CaixaBank nunca solicitará por teléfono, SMS o correo electrónico información sobre contraseñas, datos personales o claves. La entidad trabaja continuamente en proporcionar información de seguridad a sus clientes, manteniendo actualizada la sección de seguridad del sitio web. Ante cualquier solicitud sospechosa, se recomienda a los clientes contactar inmediatamente con el número de Atención al Cliente de CaixaBank (900 40 40 90).