Vishing: ¡Hola, llamo a robarte!

El *vishing* en un tipo de fraude que se realiza por medio de una llamada telefónica, es una de las formas que utilizan los delincuentes para obtener datos personales de cuentas bancarias.

Un supuesto empleado de una entidad se comunica ofreciendo supuestos servicios o productos para los cuales requieren los datos personales y los de tarjeta para realizar la venta o confirmar los datos por medio de un sitio web**,** a la que facilitan un enlace mediante un mensaje de texto.

Las entidades financieras, jamás solicitan datos personas o de sus productos mediante correo electrónico, mensajes de texto o llamadas telefónicas, excepto cuando es el cliente quien se comunica para aclarar alguna situación.

¡Siga estas recomendaciones y manténgase alerta!

- **No suministre información confidencial como respuesta a un correo electrónico o a una llamada telefónica**. Las entidades financieras jamás se contactarán con una persona para solicitar información sensible y

confidencial sobre claves y contraseñas. No existe ninguna vía autorizada para pedir esa información.

- Solicite el nombre de la organización, el nombre completo de la persona que llama, el cargo y número para devolver la llamada. **Contacte a la organización directamente, usando la información que se encuentra en el su sitio web oficial de esa entidad, para determinar si la llamada era legítima.**

- En las tiendas de aplicaciones de dispositivos móviles se puede encontrar aplicaciones (*apps*) que brindan servicios de rastreo de llamadas que permiten identificar y bloquear llamadas provenientes de fuentes desconocidas o sospechosas. Y de esta forma estar prevenido.