Superintendencia de Bancos
Guatemala, C. A.

La Superintendencia de Bancos

informa que:

Derivado de la proliferación de las tecnologías de información en la prestación de los servicios financieros, se ha acentuado recientemente la comisión de estafas por medios electrónicos dirigidos principalmente a los usuarios de dichos servicios.

Dentro de las estafas por medios electrónicos más comunes se encuentran:

- Las técnicas de **ingeniería social**, especialmente ***phishing,*** que es un proceso en el que los delincuentes, a través de engaño, obtienen información de los usuarios con el fin de estafarlos.
- La clonación de tarjetas y la tipología ***carding*** (información de tarjetas de crédito o débito comprometida en la *Dark* y *Deep Web*, que luego es vendida para cometer fraudes).
- El ***SIM Swapping***, que ha venido cobrando relevancia a nivel local, que consiste en que previo a la obtención de información personal de los usuarios a través de engaño, los ciberdelincuentes mediante usurpación de identidad logran obtener el chip del teléfono móvil del usuario, para luego cometer la estafa en contra de este, tomando el control de su banca digital.
- El **robo de los dispositivos electrónicos**, en algunos casos los delincuentes cuentan con tecnología para identificar patrones de desbloqueo de los dispositivos. Una vez desbloqueado el dispositivo pueden adicionar su rostro o huellas, para luego realizar operaciones ilícitas en las bancas en línea o aplicaciones móviles.

Es importante comentar que, el **eslabón principal de las estafas por medios electrónicos cometidos contra usuarios se desencadena a través de los propios usuarios,** quienes brindan a terceros, por desconocimiento, falta de validación o por excesiva confianza, su información a través de los diferentes canales de Internet (correo electrónico, mensajes de texto, redes sociales o incluso vía telefónica).

La Superintendencia de Bancos ha realizado esfuerzos, en el ámbito de su competencia, para fortalecer la gestión en materia de seguridad de la información y ciberseguridad, dentro de los cuales se puede mencionar:

- Seguimiento al cumplimiento de las regulaciones prudenciales y a la gestión adecuada de los riesgos operacional y tecnológico.
- Participación en el Comité Nacional de Seguridad Cibernética (CONCIBER), presidido y coordinado por la Secretaría de Inteligencia Estratégica del Estado (SIE).
- Iniciativa de Ley de Ciberseguridad, propuesta emitida por CONCIBER, con el apoyo en su elaboración por parte de BANCERT-ABG, grupo integrado por los Oficiales de Seguridad de la Información (CISO´s), MINEX, MINDEF, MINGOB, entre otros. Esta iniciativa de ley se encuentra en la Secretaría General de la Presidencia del Gobierno de la República de Guatemala, desde noviembre de 2023, a la espera de que bajo los procedimientos establecidos sea sometida a lectura y aprobación por el Congreso de la República.
- Coordinación con la Fiscalía de Delitos Transnacionales y la Intendencia de Verificación Especial, a través de la instalación de una mesa de trabajo sobre estafas, derivado de lo cual se han presentado al Ministerio Público en 2023, 38 denuncias y ampliaciones de denuncias sobre estafas, que ascienden a un monto de Q319.52 millones.
- Seguimiento como mediador, a través de la Unidad de Atención a los Usuarios de la SIB, a las quejas recibidas de los usuarios por situaciones no resueltas por parte de los bancos, principalmente por cargos no reconocidos o fraudes.
- Las entidades bancarias y el ente supervisor realizan campañas de concientización y educación financiera, con el objeto de contribuir a mitigar el cibercrimen.

Finalmente, la Superintendencia de Bancos reitera a la población su llamado a no dejarse sorprender para evitar ser víctimas de estafas por medios electrónicos y atender las recomendaciones de seguridad:

- Escribir uno mismo la dirección web de la banca electrónica de su banco.
- No ingresar a la banca en línea desde correos electrónicos, mensajes de texto o enlaces que se reciban por WhatsApp.
- No compartir su información o credenciales por mensaje de texto, WhatsApp o llamada telefónica.
- Si se recibe alguna comunicación sospechosa, contactar a su banco a través de sus canales oficiales.
- Denunciar ante las autoridades competentes.

Trabajamos para promover la estabilidad y confianza en el sistema financiero supervisado.

Visite www.sib.gob.gt