Superintendencia del Sistema Financiero

GOBIERNO DE EL SALVADOR

ALERTAS

septiembre de 2020

Método de **Estafa**	Mensajes que **buscan confundir al público**	**RECOMENDACIONES**
1. CRÉDITO EXPRÉS		
• Otorgamiento de crédito de forma inmediata. • Crédito de fácil acceso y sin garantía. • Muestran compromiso en brindar el apoyo al usuario. • Presentan información distorsionada al usuario, pretendiendo ser una institución reconocida del sistema financiero.	• Utilizan alguna insignia o distintivo, que **parece ser de una entidad supervisada**. • Utilizan **nombres similares a los de las entidades financieras** supervisadas, para confundir a los posibles deudores. • Solicitan **información y pagos anticipados al posible deudor**, para agilizar su trámite.	• Verifica que la **entidad** con la que realizas el crédito **esté autorizada**. • Ninguna entidad financiera **te solicitará dinero** previo al desembolso del crédito. • Antes de realizar cualquier operación financiera, **investiga si la entidad es confiable**, y de ser el caso, confirma si dicha entidad es realmente supervisada por la SSF. • Antes de hacer alguna transacción con estas entidades financieras, asesórate en nuestra página web si la entidad está registrada como entidad supervisada.
• Correos electrónicos con dominios similares a los de entidades financieras o de instituciones de Gobierno, que expresan que se tiene algún problema de pago de sus obligaciones.	• Utilizar formatos en el mensaje de correo, similares al de entidades financieras o de instituciones de Gobierno, en el cual **remiten vínculos donde se solicita información personal,** para la solución del problema de impago.	• No compartir información personal por medios electrónicos con fuentes desconocidas. • Valida las direcciones de correos electrónicos con sospecha de que pueden ser falsos y tengan como objetivo obtener información personal y de tus cuentas. • Antes de proceder a brindar cualquier información, llama a la entidad o institución de Gobierno para verificar la veracidad del correo o los mensajes de texto recibidos.

Superintendencia del Sistema Financiero

GOBIERNO DE EL SALVADOR

ALERTAS

septiembre de 2020

Método de **Estafa**[1]	Mensajes que **buscan confundir al público**	**RECOMENDACIONES**
2. VISHING / SMISHING		
• Llamadas o mensajes al teléfono celular con aviso de haber sido ganador de un premio. • Llamadas del "banco" para indicar un posible fraude.	• Se hacen pasar por ejecutivos de entidades financieras. • Remiten mensajes SMS como si fueran una entidad financiera, al responder el usuario solicitan información personal y transferencias bancarias para reclamar su premio. • Solicitan datos personales y claves para poder efectuar el posible fraude.	• Si tienes dudas respecto del premio a entregar a nombre de una entidad financiera o de la manera con la cual has obtenido un premio, confirma que la información provenga de fuentes confiables. • Recuerda que las instituciones financieras no te requerirán una transferencia bancaria para otorgar un premio. • La entidad financiera no te solicitará claves, por medios telefónicos, mensajería o correos electrónicos.
3. SPAM		
• Correos electrónicos de supuestos inversionistas extranjeros que buscan colocar o depositar sus fondos. • Los mensajes también pueden llegar a tu teléfono celular.	• Aparentemente, se trata de personas que han ganado la lotería o se han hecho acreedoras de millonarías herencias, y están dispuestas a invertirlas o depositarlas, ofreciendo jugosas comisiones a quienes proporcionen información personal en los vínculos adjuntos al correo electrónico. Los vínculos también pueden llegar a través de mensajes de texto en tu teléfono celular.	• No compartas información personal de fuentes desconocidas. • Valida las direcciones de correos electrónicos que puedan ser falsos y tengan como objetivo obtener información personal y de tus cuentas. Esto también puede ocurrir a través de mensajería en tu teléfono celular.
4. FRAUDE EN COMERCIO ELECTRÓNICO		
• Sitios web de compras con precios mucho más bajos que los del mercado o comercios.	• Sitios web que ofrecen precios atractivos, de productos de marcas reconocidas, para los consumidores. • Sitios web con URL que parece ser confiable, haciendo uso de una denominación similar a un comercio reconocido. • Ventanas emergentes que muestran mensajes de Error y le piden dar "clic aquí" para solucionarlo.	• Al hacer tus compras en línea, verifica que las estás realizando en un sitio web seguro, el cual podrás identificar por medio de https//: o el ícono de un candado cerrado, al inicio de la dirección. Si tienes sospechas que el sitio no es confiable, no la realices. • Revisa los comentarios de los usuarios, de esa forma podrás también tener idea si se trata de una estafa.

Superintendencia del Sistema Financiero

GOBIERNO DE EL SALVADOR

ALERTAS

septiembre de 2020

Método de **Estafa**[1]	Mensajes que **buscan confundir al público**	**RECOMENDACIONES**
5. PHISHING		
• Técnica que persigue engañar a un usuario haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar. • Sitios web que parecen de entidades autorizadas. • Utilizan URL similares al de la institución autorizada.	• Sitio web similar al de una entidad autorizada, ya que contemplan los colores y marca de entidades financieras reconocidas.	• Al realizar una consulta u operación electrónica, asegurate que utilizas el canal de atención oficial de la institución autorizada; esto te garantiza que la atención está siendo brindada por personas autorizadas, dándote seguridad en el manejo de tu información. • No ingreses información personal o financiera por medio de los enlaces de la entidad financiera no autorizada.
6. MALWARE		
• Vínculos en internet, correo electrónico, o en tus dispositivos móviles a través de mensajes de texto, remiten virus para robo de información.	• El texto del correo o mensaje en internet,induce a que el usuario haga clic en un vínculo, ya sea para visitar una página o descargar un archivo; automáticamente el vírus descarga la información personal y financiera que se tiene almacenada en el dispositivo electrónico.	• Recuerda no darle autoguardado a datos de tarjetas de crédito, acceso a cuentas en línea con entidades financieras o comercios; ingrésalos tú mismo en cada transacción que realices.