BANCA MIFEL, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE, GRUPO FINANCIERO MIFEL, (en adelante "MIFEL"), así como sus directores, funcionarios y empleados no serán responsables en caso de pérdida, daño (ya sea directo o indirecto) y/o gastos de cualquier naturaleza que se pueda atribuir como resultado del uso de cualquier información, enlace o servicio proporcionado a través de este sitio web, eximiéndolos de toda la responsabilidad frente a terceros. Sin limitar lo anterior, la información provista en este sitio web tiene la intención de proporcionarle a usted, el usuario, información objetiva sobre los servicios financieros de MIFEL y no pretende constituir una recomendación, guía o propuesta con respecto a la idoneidad de algún producto con respecto a cualquier necesidad financiera que pueda tener. Cualquier material descargado u obtenido de otro modo a través del uso de este sitio se realiza bajo su propia discreción y riesgo y el usuario será el único responsable de cualquier daño a su sistema informático o pérdida de datos que resulte de la descarga de dicho material. Ningún consejo o información, ya sea oral o escrito, obtenida por el usuario de MIFEL creará ninguna garantía que no estén expresamente establecidos en los términos y condiciones puestos a disposición del usuario. Aunque se han realizado todos los esfuerzos para garantizar la seguridad en los servicios de MIFEL, el equipo de MIFEL advierte a todas las personas que desean usar los Servicios y Productos que ofrece y proporciona MIFEL, que existen muchos métodos que los ciberdelincuentes usan para tratar de obtener datos personales para cometer varios fraudes. Los más importantes son:

a) Phishing: En Internet, "phishing" se refiere a actividades delictivas que intentan obtener información confidencial de manera fraudulenta. Hay varias formas en que un estafador puede tratar de obtener información confidencial. A veces, un defraudador envía un correo electrónico benigno para atraerlo a una conversación y luego seguir con un correo electrónico de phishing. En otras ocasiones, el estafador solo enviará un correo electrónico de suplantación de identidad (phishing) que lo dirigirá a un sitio web en el que se le pedirá que ingrese su información personal, como su nombre de usuario y contraseña.

b) Pharming: Es otra estafa en la que un defraudador instala un código malicioso en una computadora personal o servidor. Este código luego redirige los clics que hace en un sitio web a otro sitio web fraudulento sin su consentimiento o conocimiento.

c) Vishing: Desafortunadamente, los correos electrónicos de phishing no son la única forma en que las personas pueden intentar engañar para que proporciones información personal en un esfuerzo por robar tu identidad o cometer fraude. Los estafadores también usan el teléfono para solicitar información personal.

d) Smishing: Al igual que el phishing, smishing utiliza mensajes de texto en el celular para atraer a los consumidores. A menudo, el texto contendrá una URL o número de teléfono. El número de teléfono a menudo tiene un sistema automático de respuesta de voz. Y de nuevo, al igual que el phishing, el mensaje de smishing normalmente solicita su atención inmediata.

Por lo tanto, es responsabilidad del usuario acatar todas las medidas para evitar los fraudes cibernéticos.