EDUCACIÓN FINANCIERA EN TU INSTITUCIÓN

¡INFÓRMATE Y PROTÉGETE DE LOS FRAUDES!

Dada la facilidad que existe de encontrar a alguien con WhatsApp tras escribir un número de teléfono cualquiera, los fraudes a través de este medio son cada vez más comunes.

¿Cómo se inicia la estafa?

A través de un SMS o mensaje de texto, los ciberdelincuentes registran o asocian el número de teléfono celular de su víctima a una cuenta de WhatsApp en otro teléfono celular.

Inmediatamente, sin haber hecho nada, vas a recibir una notificación de WhatsApp en tu teléfono con el siguiente mensaje: ***"Tu número de teléfono ya no está registrado en este dispositivo. Esto probablemente se debe a que registraste tu número en un teléfono diferente. Verificar".***

Entonces los estafadores envían un mensaje afirmando que la aplicación no está actualizada y que para seguir utilizando el servicio se deberá verificar la cuenta a través de un código de seis dígitos que llegará por SMS que deberás compartirles.

Cuando envías el código de verificación recibido, los delincuentes podrán acceder a tu cuenta de WhatsApp en otro dispositivo, y a partir de allí, la cuenta de WhatsApp en tu celular se bloqueará y te llegará un mensaje advirtiéndote que tu cuenta ya no está vinculada a tu teléfono.

Durante el tiempo en el que intentas recuperar tu cuenta, los defraudadores podrán ingresar a tu lista de contactos y a tu historial de chats, con la finalidad de estafar a tus contactos solicitándoles transferencias de dinero haciéndose pasar por ti.

Para evitar que otras personas entren a tu cuenta en otro dispositivo y tengan acceso a tus conversaciones y contactos, es recomendable activar la verificación en dos pasos. Y para ello sigue estas sencillas recomendaciones

1. Ingresa a WhatsApp y ve a la opción "Ajustes".
2. Da clic en "Cuenta" y selecciona "Verificación en dos pasos".
3. Elige "Activar" y establece un PIN de seguridad.
4. Confirma el PIN, ingresa tu correo electrónico y ¡Listo!

Ante cualquier sospecha de delito o ataque cibernético, repórtalo en la Secretaría de Seguridad y Protección Ciudadana, al correo **ceac@sspc.gob.mx.** En la Ciudad de México este tipo de mensajes sospechosos o fraudulentos pueden denunciarse directamente a la Policía Cibernética de la CDMX, mediante su Twitter **@SSC_CDMX** o en el correo electrónico **policia.cibernetica@ssp.cdmx.gob.mx**.