10 Diez consejos para evitar el fraude cibernético:

1. Tenga cuidado con los correos electrónicos que contengan documentos y archivos adjuntos; los archivos podrían tener un virus.
2. Evite llenar formularios incluidos en mensajes de correo electrónico que le pidan su información personal.
3. No conteste un correo electrónico no solicitado (spam) o mensajes en ventanas emergentes que le pidan información personal o financiera.
4. No haga clic en vínculos de un correo electrónico no solicitado.
5. Si recibe un correo electrónico que señala que es de una empresa con la que usted tiene negocios, contacte directamente a la empresa para verificar que el correo sea genuino.
6. En lugar de hacer clic en el vínculo del correo no solicitado, inicie sesión directamente en el sitio web oficial de la empresa identificada en el correo electrónico.
7. Si el correo electrónico parece ser de su banco o su cooperativa de crédito, de un emisor de tarjetas de crédito o de otra empresa con la que trata con frecuencia, tenga cuidado y no haga clic ni responda al correo electrónico. Usted puede encontrar la información oficial o legitima del negocio o banco en sus reportes bancarios. Las instituciones financieras no solicitan información personal via correo electrónico.
8. Los hotspots de Wi-Fi ofrecen acceso gratuito a la Internet, se encuentran con frecuencia en cafeterías, bibliotecas, aeropuertos, hoteles, universidades y otros lugares públicos. Aunque son convenientes, las redes públicas de Wi-Fi con frecuencia no son seguras. Proteja su información personal mientras usa las redes públicas inalámbricas.
9. Evite exponer información privada, como sus nombres de usuario, contraseñas y número de Seguro Social.
10. Si un hotspot de Wi-Fi no le solicita una contraseña, entonces no es seguro. Otros usuarios en la red pueden ver lo que envía. Pueden tener acceso a su información personal, documentos privados, hasta a su identificación para iniciar sesiones sin su conocimiento o permiso.