SAN BERNARDINO COUNTY | Aging and Adult Services

ALERTA DE ESTAFA

Estafa: Mensajes de Limite de Almacenamiento de Datos Dirigida a: Personas Mayores

Estafadores pueden enviarle un correo electrónico con mensaje que parece ser de su proveedor de internet, compañía de teléfono celular, o compañía de seguridad de computadora. Normalmente, la línea de asunto del correo electrónico indicara "Actualización Requerida", y el mensaje indicará que usted ha alcanzado su límite de almacenamiento de datos. Los estafadores utilizarán tácticas de miedo tales como, "Si usted no se actualiza, será bloqueado de mandar o recibir correos electrónicos y sus fotos y documentos no se guardarán." El mensaje le indica que haga clic en el enlace que se puede parecer a su dirección de correo electrónico, pero en su lugar le vincula a un sitio de web en el extranjero y le pedirá que complete un formulario que incluye su información personal. ¡Este formulario lo hará vulnerable al robo de identidad!

¡Un enlace en un correo electrónico puede llegar al robo de indentidad!

La Oficina de Buenas Prácticas Comerciales (BBB) ofrece estas sugerencias para evitar este tipo de estafa:

- **Sea consciente de correos electrónicos o mensajes de texto inesperados que contienen enlaces o archivos adjuntos:** No haga clic en los enlaces o abra archivos si usted no reconoce al remitente.
- **Recuerde que las apariencias pueden ser engañosas:** Los estafadores son capaces de falsificar cualquier cosa desde el logotipo de una empresa hasta un correo electrónico. Simplemente porque un correo electrónico parece real, no significa que es real.
- **Consulte con su proveedor de servicio de Internet o teléfono celular:** Si algo suena sospechoso, confirme primero su legitimidad. Comuníquese con ellos directamente usando un número que usted sabe que es exacto, no de cualquier enlace o número proporcionado en el correo electrónico o mensaje de texto sospechoso.
- **Tenga cuidado con correos electrónicos genéricos:** Los estafadores utilizan a menudo poca o ninguna información específica para animarle a abrir el mensaje para los detalles.
- **Cuestione mensajes conteniendo poca o ninguna información personal:** Los estafadores a menudo obtienen información parcial o incorrecta para engañarlo a proporcionar la información correcta pidiéndole que "actualice y confirme"
- **Utilice contraseñas únicas:** Utilice contraseñas diferentes para cada cuenta que usted crea. Esta es una manera simple de reducir su riesgo si una contraseña cae en las manos de los estafadores.

Si usted piensa que ha sido victima de una estafa, póngase en contacto con Servicios de Protección para Adultos (APS) del Condado de San Bernardino al 877-565-2020, o su departamento de policía local.