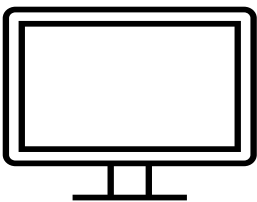


¿QUÉ ES UNA ESTAFA DE HACKER FANTASMA?



El FBI advierte al público de un reciente aumento a nivel nacional de las estafas de "hacker fantasma", que afectan significativamente a las personas mayores. Estas estafas son una evolución de las estafas de apoyo técnico más generales que usan una combinación de impostores de apoyo técnico, instituciones financieras y gubernamentales para aumentar la confianza que las víctimas depositan en los estafadores e identificar las cuentas más lucrativas a las que apuntar. Las víctimas a menudo sufren la pérdida de cuentas bancarias, de ahorro, de jubilación o de inversión completas con el pretexto de la "protección" de sus activos.

ESTAFA DE HACKER FANTASMA



Impostor de apoyo técnico

- Finge ser apoyo técnico
- Le indica que instale software en su computadora para permitirle acceder de forma remota
- Puede observar las finanzas en general



Impostor de institución financiera

- Indica que su computadora y cuentas financieras han sido pirateadas
- Le indica que mueva dinero a una entidad del gobierno de los Estados Unidos, como la Reserva Federal, por "seguridad"



Impostor del gobierno de los Estados Unidos

- Se hace pasar por empleado del gobierno
- Puede proporcionar membretes de aspecto oficial para parecer legítimo.

SIGUE



**Línea directa nacional contra el fraude a las
personas mayores
1-833-372-8311**

¿QUÉ ES UNA ESTAFA DE HACKER FANTASMA?



El FBI está advirtiéndole al público sobre un aumento a nivel nacional de las estafas de "hackers fantasma", que afectan significativamente a las personas mayores. Estas estafas son una evolución de las estafas de apoyo técnico más generales que usan una combinación de impostores de apoyo técnico, instituciones financieras y gubernamentales para aumentar la confianza que las víctimas depositan en los estafadores e identificar las cuentas más lucrativas a las que apuntar. Las víctimas a menudo sufren la pérdida de cuentas bancarias, de ahorro, de jubilación o de inversión completas con el pretexto de la "protección" de sus activos.

PROTÉJASE

-  No haga clic en ventanas emergentes no solicitadas, enlaces enviados por medio de mensajes de texto o enlaces o archivos adjuntos de correo electrónico.
-  No se comunique con el número de teléfono proporcionado en una ventana emergente, mensaje de texto o correo electrónico.
-  No descargue software por solicitud de un individuo desconocido que se comunicó con usted.
-  No permita que un individuo desconocido que se comunicó con usted obtenga control de su computadora.
-  El gobierno de los EE. UU. nunca le solicitará que envíe dinero mediante transferencia electrónica a cuentas extranjeras, criptomonedas o tarjetas de regalo/prepagadas.

DENÚNCIELO

-  Denuncie actividades fraudulentas o sospechosas a la oficina local del FBI y a FBI IC3 en www.ic3.gov.
-  Sea lo más detallado posible en su informe e incluya: nombre de la persona o empresa que se comunicó con usted, números de cuentas bancarias donde se realizaron las transferencias bancarias y nombre del beneficiario, números de teléfono, sitios web, etc.

SIGUE



**Línea directa nacional contra el fraude a las
personas mayores
1-833-372-8311**