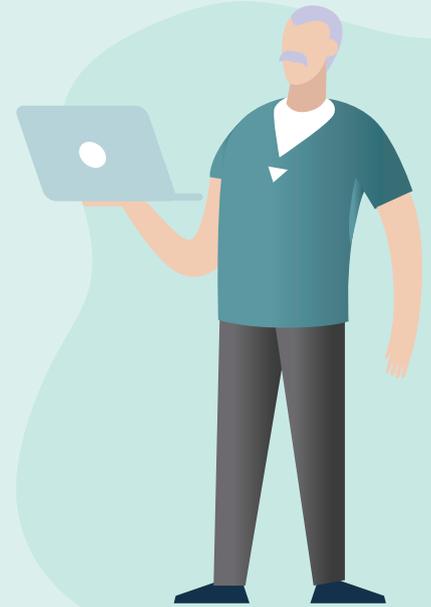


Protéjase de las estafas

Una estafa es una actividad ilegal o deshonesta que engaña a las personas para dar dinero, información personal, imágenes íntimas o cualquier otra cosa de valor. Una estafa en línea normalmente la comete alguien con un perfil falso o un negocio fraudulento. Así que, aunque Internet puede ser un lugar estupendo para explorar, merece la pena ser cauteloso.

Ser consciente de que hay estafadores es uno de los primeros pasos para evitarlos. Una vez que conozca sus timos, tendrá más probabilidades de detectar las estafas. Estar alerta siempre es la mejor defensa.

Aquí encontrará algunos consejos para reconocer y evitar las estafas.



Proteja su información personal

Los estafadores intentan acceder a su información personal haciéndole preguntas o dándole indicaciones por una llamada de teléfono, un correo electrónico, un mensaje de texto o las redes sociales. Los estafadores utilizarán sus datos personales para robarle dinero o cometer otro delito.

¿Qué piden los estafadores?

Los estafadores intentan ganarse su confianza haciéndose pasar por miembros de una organización o agencia reconocida como NBN Co, Telstra, Microsoft, Australia Post, los servicios fiscales, la policía o Services Australia (MyGov, Centrelink, Medicare).

Con el fin de engañarle para que dé su información personal o financiera, los estafadores pueden:

- hacer que pinche en un enlace
- pedirle que les dé acceso remoto a su computadora
- pedirle que pague una deuda
- pedirle que compre un cupón para pagar una multa
- pedirle que transfiera fondos o envíe dinero al extranjero

Señales de que puede ser una estafa

Preste atención a:

- correos electrónicos, mensajes o llamadas que no espera o que proceden de alguien que no conoce
- promesas sobre beneficios económicos
- amenazas de multas o deudas
- amenazas de cerrar o bloquear su cuenta
- enlaces que no parecen verdaderos, como tener una dirección web poco usual
- un plazo o un sentido de urgencia inusuales

Consejo: no utilice los datos de contacto facilitados si no está seguro de si un mensaje o llamada es real, en su lugar busque en Internet el número o la dirección de correo electrónico de la organización.

Tenga cuidado con los amigos que ha hecho en Internet

Los estafadores de Internet suelen ponerse en contacto con personas a través de las redes sociales. Utilizan sus tácticas en estafas sobre citas y de buscar pareja. También abordan a personas que juegan en Internet a juegos como Palabras con amigos (Words with Friends) y el Scrabble. Su objetivo es establecer una relación (no tiene por qué ser amorosa) para ganarse su confianza y pedirle así dinero, información personal, imágenes íntimas o cualquier otra cosa de valor.

Señales de que puede ser una estafa

Preste atención a personas que:

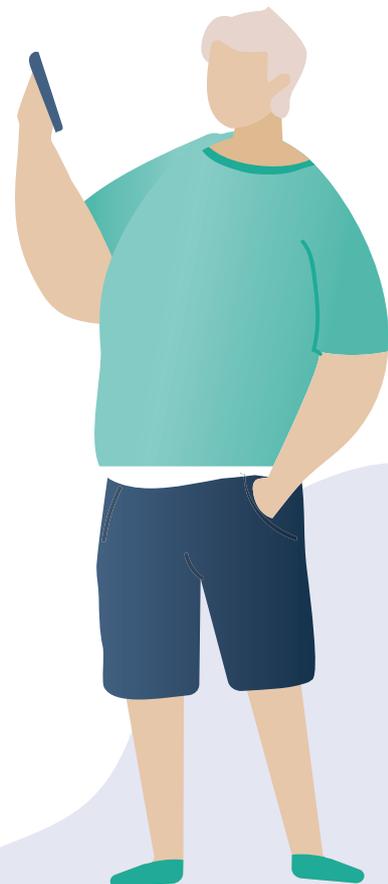
- expresan mucho afecto rápidamente
 - intentan trasladar la conversación del sitio web donde se conocieron a un canal de comunicación más privado, como el correo electrónico o los mensajes directos
 - le cuentan historias elaboradas sobre problemas financieros
 - le dicen que quieren quedar con usted pero le ponen excusas, o que le piden dinero para así poder "viajar" y conocerle
 - le preguntan sobre su situación económica
 - son persistentes, más directos o incluso agresivos cuando no envía el dinero
 - parecen tener datos incoherentes en su perfil de Internet; por ejemplo, su foto parece diferente a su descripción o dicen que han estudiado en la universidad, pero su gramática es incorrecta.
- No haga ningún pago por giro bancario, transferencia bancaria, transferencia internacional de fondos o monedas electrónicas como el bitcoin. (Es muy difícil recuperar el dinero enviado de esta manera si resulta que al final ha sido una estafa).
 - No acepte entregar paquetes internacionales ni transferir dinero para otra persona, porque puede estar cometiendo un delito sin saberlo.
 - No comparta fotos íntimas ni utilice las webcams en un entorno privado.
 - Corte todas las comunicaciones si una persona empieza a pedirle dinero o un favor.
 - Esté pendiente de errores ortográficos, gramática incorrecta e incoherencias en las historias.

También es muy común que los estafadores finjan ser trabajadores humanitarios o se hagan pasar por personal militar o profesionales que trabajan en el extranjero.

Consejo: haga una búsqueda de imágenes en páginas como Google (images.google.com) o Tineye (tineye.com) para ayudarle a comprobar si la persona es quien dice ser.

Cómo protegerse

- No proporcione información personal o financiera a gente que nunca ha conocido en persona.



Preste atención a las estafas de inversiones

Los estafadores de inversiones dedican mucho tiempo, esfuerzo y dinero a crear historias convincentes, sitios web sofisticados y folletos vistosos para estafar a las personas mayores de Australia que parecen haber aumentado su "hucha" o sus ahorros.

¿Cómo consiguen su atención los estafadores?

Estos son algunos de los métodos que emplean los estafadores de inversiones:

- Le dirigen a un sitio web falso que hace afirmaciones fraudulentas sobre inversiones con muy buenos resultados y beneficios.
- Publican un anuncio o artículo en la página de una red social como Facebook.
- Le envían una petición de "amistad" en las redes sociales haciéndose pasar por alguien que conoce o al que está conectado en las redes, para así acceder a la información de su perfil y enviarle ofertas personalizadas en las que invertir.

Señales de que puede ser una estafa

- El estafador le llama o le envía correos electrónicos constantemente.
- Pasan su llamada a otra línea: primero le habla una persona joven y después una persona más mayor intenta cerrar el trato.

- Le presionan para que actúe con rapidez o de lo contrario perderá su oportunidad de inversión.
- Afirman que no tienen una licencia de los Servicios Financieros de Australia (AFS) o que no necesitan una.
- Intentan que no se retire del trato.



Plan de jubilación

Los estafadores de inversiones ofrecen formas rápidas y fáciles para "desbloquear" de manera anticipada su dinero del plan de jubilación (superannuation). Pueden pedirle que acepte una historia para garantizar así la disposición anticipada de su dinero y después, actuando como su asesor financiero, engañan a la empresa que gestiona su plan de jubilación para que le pague sus beneficios directamente a ellos.

Cuando ya tiene su dinero, el estafador puede llevarse unas "comisiones" cuantiosas del fondo desbloqueado o dejarle sin nada de dinero.



¡Nota! normalmente no puede acceder de manera legal a la parte destinada a su plan de jubilación hasta que no tenga entre 55 y 60 años, dependiendo del año en el que haya nacido. Hay determinadas excepciones como dificultades económicas graves o razones humanitarias, pero cualquiera que ofrezca otra forma de acceder a su plan de jubilación actúa de manera ilegal.

Inflar artificialmente el precio de acciones

Los estafadores de inversiones compran acciones a un precio bajo en una empresa pequeña, después envían consejos falsos sobre las buenas expectativas de la empresa. El precio de las acciones incrementa a medida que invierten más personas, y los estafadores venden sus acciones en el pico de la subida de precios. Entonces, el precio de la acción disminuye y los accionistas se quedan con ellas a un valor reducido.

Estafas de apoyo a famosos

Los estafadores de inversiones utilizan un apoyo falso de famosos o empresarios exitosos y respetados en un intento por atraer a personas para que crean en un programa que está respaldado por alguien en quien confían. Estas estafas suelen aparecer en anuncios de Internet, en historias promocionales en redes sociales o en sitios web que parecen auténticos y fiables.

Cómo protegerse

- Sospeche de oportunidades que parecen ser demasiado buenas para ser verdad.
- Sospeche de historias o anuncios con apoyo de famosos.
- No permita que nadie le presione.
- Si tiene menos de 55 años, preste atención a las ofertas que promocionan un acceso fácil a los beneficios del plan de jubilación.
- Investigue por su cuenta y busque asesoramiento financiero o jurídico independiente y fiable.

- No proporcione información personal o financiera hasta que:
 - haya comprobado si el asesor financiero y su empresa están registrados en el sitio web de ASIC: asic.gov.au/online-services/search-asics-registers/.
 - haya comprobado la lista de empresas de ASIC con las que no debe tratar: moneysmart.gov.au/scams/companies-you-should-not-deal-with.

Ayuda, sospecho que me han estafado

Si piensa que ha sido víctima de un fraude, no se avergüence ni lo mantenga en secreto. Hay pasos que puede seguir para solucionar el problema:

- Contacte con su banco para detener cualquier otro pago hacia el estafador.
- Contacte con ID Care idcare.org si su información personal se ha visto expuesta o la han usurpado.
- Para cualquier estafa de Medicare, Centrelink o myGov, contacte con Services Australia en el teléfono 1800 941 126 o por correo electrónico en reportascam@servicesaustralia.gov.au.
- Reporte el fraude a la Australian Competition and Consumer Commission (Comisión Australiana de Competición y Consumidores) en scamwatch.gov.au para que ellos puedan decirles a otras personas cómo evitarlo.

Para estar al día de los últimos fraudes a evitar, suscríbase a las alertas de correo electrónico de Scamwatch en scamwatch.gov.au/news/subscribe-to-scam-alert-emails

Dedique tiempo a descubrir Be Connected

Be Connected es un sitio web exhaustivo con recursos gratuitos diseñados específicamente para ayudar a las personas mayores de Australia a conectarse a Internet de manera segura y a navegar con confianza por el mundo digital. El sitio también es útil para las familias y las organizaciones comunitarias que quieren ayudar a los miembros de la comunidad de personas mayores a acceder a todos los beneficios de Internet.

beconnected.esafety.gov.au

