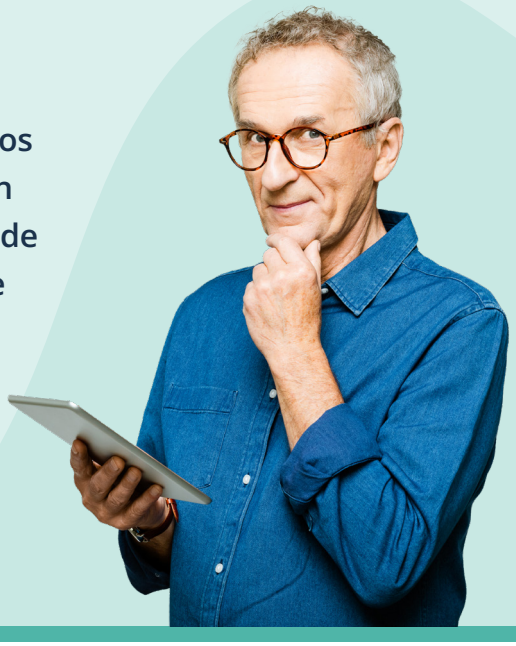
Resumen presentación web

Australian Government

Be Connected
Every Australian online.

Protéjase contra las estafas



Los estafadores son cada vez más sofisticados en sus intentos de obtener su dinero o sus datos personales. Las estafas van dirigidas a personas de todos los orígenes, edades y niveles de ingresos de toda Australia. Las estafas por Internet las suele cometer alguien que tiene un perfil o empresa falsos o que finge ser de una organización conocida. Por ello, aunque Internet puede ser un lugar estupendo para explorar, ¡vale la pena ser precavido! Esté alerta y protéjase de las estafas siguiendo nuestros consejos.

Proteja su información personal

Los estafadores se hacen pasar por organizaciones que usted conoce y en las que confía, como empresas con las que suele tratar, agencias del gobierno o algún servicio de lucha contra el fraude, para tratar de que revele información personal y financiera importante. Pueden ponerse en contacto con usted por teléfono, correo electrónico, mensaje de texto o a través de las redes sociales. Los estafadores utilizarán sus datos personales para robarle dinero o cometer otro delito.

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

- que verifique su identidad o actualice sus datos
- que haga clic en un enlace
- que les dé acceso remoto a su computadora
- que pague una deuda
- que compre un cupón para pagar una multa
- que transfiera fondos o envíe dinero al extranjero.

Señales de que puede ser una estafa

- correos electrónicos, mensajes o llamadas que no espera o que proceden de alguien que no conoce
- promesas de 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 límite de tiempo o un sentido de urgencia inusuales

Recuerde: los estafadores pueden tratar de jugar con sus emociones para hacerle reaccionar y que no se tome tiempo para pensar detenidamente sobre la situación. Algunas de las tácticas que usan son las amenazas o multas, decirle que se ha producido un gasto no autorizado desde su cuenta o hacerse pasar por un familiar que necesita ayuda.

Cómo protegerse

- Esté alerta ante la existencia de estafas y piense siempre en la posibilidad de que un mensaje, correo electrónico o llamada telefónica pueda ser una estafa.
- Sepa con quién está tratando. Si no está seguro de que un mensaje o llamada sean reales, no utilice los datos de contacto facilitados. En su lugar, busque en Internet el número o la dirección de correo electrónico de la organización.
- No proporcione información personal o financiera.
- No abra mensajes sospechosos ni ventanas emergentes, ni haga clic en enlaces o archivos adjuntos de correos electrónicos: bórrelos.
- No responda a llamadas telefónicas relativas a su computadora pidiéndole acceso remoto: cuelgue, aunque mencionen una empresa conocida, como Telstra.

Cuidado al hacer amistades en Internet

Normalmente, los estafadores se ponen en contacto con las personas a través de las redes sociales, un sitio de citas o incluso a través de un juego en línea. Se mostrarán muy amables e interesantes y estarán deseando entablar una amistad o relación con usted. Los estafadores pueden ser sorprendentemente pacientes. La falsa relación puede durar semanas o incluso un año, con el fin de ganarse su confianza y pedirle dinero, información personal o imágenes íntimas, o bien engañarle para que haga algo ilegal.

Señales de que puede ser una estafa

Preste atención a las personas que:

- expresen un profundo afecto rápidamente y se pongan en contacto con usted a menudo
- no puedan reunirse en persona, o le pidan dinero para poder desplazarse para conocerle
- intenten que salga de la plataforma o aplicación en la que se conocieron y pase a un canal de comunicación más privado, como los mensajes directos o el correo electrónico.
- afirmen tener estabilidad económica, pero le pidan dinero.
- le cuenten historias rebuscadas sobre problemas económicos
- le pregunten sobre su situación económica
- se vuelvan desesperadas, persistentes, más directas o incluso agresivas cuando no les envía dinero
- parezcan tener incoherencias en sus historias y en su perfil de Internet; por ejemplo, su foto es diferente a su descripción
- cometan errores tipográficos o gramaticales
- le digan que trabajan en el extranjero (por ejemplo, como cooperantes o en el ejército).

Cómo protegerse

- No envíe nunca dinero ni facilite los datos de su tarjeta de crédito, cuentas de Internet ni copias de documentos personales importantes a alguien que no conozca personalmente.
- Haga una búsqueda de imágenes que le ayude a determinar si realmente son quienes dicen ser. Vaya a images.google.com y haga clic en el icono de la cámara.
- Desconfíe cuando esa persona le empiece a mencionar problemas de dinero o que necesita dinero para una «emergencia».
- Esté atento a errores ortográficos y gramaticales y a incoherencias en sus relatos.
- No acepte transportar paquetes de un país a otro ni transferir dinero para otra persona, ya que puede estar cometiendo un delito.
- No comparta fotos ni vídeos íntimos. Se sabe que los estafadores chantajean a sus víctimas con material comprometedor.
- Corte todas las comunicaciones si una persona empieza a pedirle dinero o un favor.
- Evite todo acuerdo con un desconocido que le pida un pago mediante giro postal, transferencia bancaria, transferencia internacional de fondos, tarjeta precargada o moneda electrónica, como Bitcoin. Es difícil recuperar el dinero que se ha enviado de esta forma.

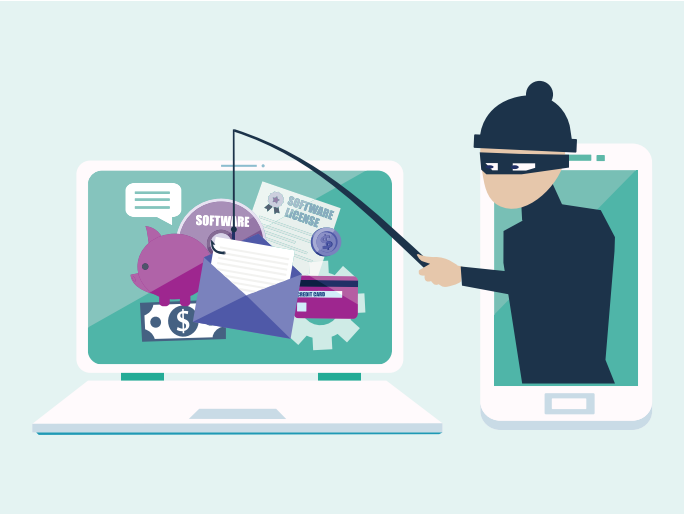
Esté atento a las estafas de inversiones

Las estafas de inversiones consisten en promesas de pagos de fuertes sumas de dinero, dinero rápido o rendimientos garantizados. Desconfíe siempre de toda oportunidad de inversión que prometa un alto rendimiento con poco o ningún riesgo.

Los australianos pierden más dinero por estafas de inversiones que por otro tipo. Pueden ser difíciles de detectar, ya que los estafadores se esfuerzan mucho por crear historias convincentes y por diseñar sitios web y materiales promocionales profesionales. Antes de invertir, solicite siempre asesoramiento jurídico o financiero independiente a un asesor financiero registrado en la Comisión Australiana de Valores e Inversiones (Australian Securities and Investments Commission, ASIC).

Algunas de las modalidades más frecuentes de estafas de inversión son:

- ponerse en contacto con usted por correo electrónico o por teléfono con una oportunidad especial de obtener una rentabilidad rápida o garantizada
- utilizar falsos avales de personas famosas para hacer que la estafa parezca legítima
- convencerle de que acceda al dinero de su fondo de jubilación de forma anticipada o en un pago único
- seminarios de inversión (a menudo por vídeo a través de Internet, Zoom o similar) que son gratuitos o cobran altas tasas de asistencia.



Fondo de jubilación (superannuation)

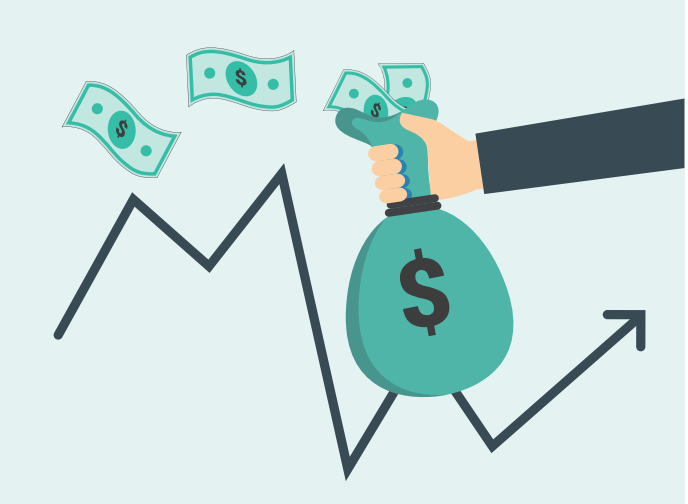
Las estafas relacionadas con los fondos de jubilación le ofrecen acceso anticipado a su fondo de jubilación, a menudo a través de un fondo de jubilación autogestionado o a cambio de una comisión. La oferta puede provenir de un estafador que se haga pasar por asesor financiero.

Pueden pedirle que acepte una historia por la que se garantiza 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.

Nota: No se suele puede acceder de manera legal a la parte preservada de su fondo 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 fondo de jubilación actúa de manera ilegal. Para obtener más información, visite: moneysmart.gov.au/how-super-works/superannuation-scams

Asesoramiento y promociones para la compra de acciones

Los estafadores pueden ponerse en contacto con usted por correo electrónico o las redes sociales o publicar un mensaje en un foro para animarlo a que compre acciones de una empresa que, según las predicciones de los estafadores, está a punto de revalorizarse. El mensaje parece ser información privilegiada y suele insistir en la necesidad de actuar con rapidez. El estafador está intentando que usted compre acciones para que aumente el precio de estas y así poder vender las acciones que ya ha comprado el estafador y obtener un alto beneficio. El valor de las acciones bajará drásticamente.



Estafas relacionadas con el apoyo de famosos

Los estafadores usan la imagen, el nombre y las características personales de famosos sin el permiso de estos para convencerle de que invierta, haciéndole ver que está respaldado por alguien en quien confía. Estas estafas suelen aparecer en forma de anuncios en Internet o historias promocionales en las redes sociales, o bien en sitios web aparentemente legítimos y fiables.

Señales de advertencia de una estafa de inversión

Alguien se pone en contacto con usted de forma inesperada a través de una llamada telefónica, un mensaje de texto, un correo electrónico o por un mensaje en las redes sociales y le ofrece asesoramiento de inversión que no ha solicitado, y esta persona:

- utiliza tácticas de alta presión, como ponerse en contacto con usted en repetidas ocasiones y presionarle para que tome una decisión rápida.
- promete riesgos bajos con rendimientos altos o garantizados.
- no tiene una licencia de los Servicios Financieros de Australia (AFS) o dice que no la necesita.
- tiene un prospecto de información al inversionista que no está registrado en la ASIC.
- utiliza imágenes o avales de famosos; estos suelen ser falsos. Los famosos rara vez hablan de sus inversiones o de sus decisiones financieras en público.
- le dirige a un sitio web falso.
- trata de impedir que cancele el trato.

Cómo protegerse

- Sospeche de las oportunidades que parecen ser demasiado buenas para ser verdad.
- Sospeche de historias o anuncios que cuentan con el 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 fondo 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 tanto el asesor financiero como la empresa están registrados. Lo puede verificar en el sitio web de la ASIC: asic.gov.au/online-services/search-asic-s-registers/
  - haya comprobado la lista de empresas de ASIC con las que no debe tratar: moneysmart.gov.au/companies-you-should-not-deal-with

Los mejores consejos para evitar estafas

Deténgase

- Tómese su tiempo antes de dar dinero o sus datos personales a nadie.
- Los estafadores le ofrecerán ayuda o le pedirán que verifique su identidad. Fingirán ser de organizaciones que usted conoce y en las que confía, como una empresa con la que suele tratar, o la policía, el gobierno o un servicio antifraude.

Piense

- Pregúntese: ¿Podría ser un mensaje o llamada falsos?
- Nunca haga clic en un enlace de un mensaje y pregunte a un amigo o familiar de confianza qué harían ellos. Solo contacte con empresas o con el gobierno usando la información de contacto del sitio web oficial o través de aplicaciones seguras. Si no está seguro, diga que no, cuelgue o elimine.

Protéjase

- Actúe con rapidez si presiente que algo no está bien.
- Póngase en contacto con su banco de inmediato si pierde dinero o información personal o si observa alguna actividad inusual en sus tarjetas o cuentas. Pida ayuda en organizaciones como IDCARE y denuncie los delitos informáticos en ReportCyber. Ayude a los demás denunciando las estafas a Scamwatch.

Ayuda, sospecho que me han estafado

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

- Póngase de inmediato en contacto con su banco o entidad financiera para detener nuevos pagos al estafador.
- Si ha sido víctima de un ciberdelito y ha perdido dinero por Internet, lo puede denunciar a la policía a través de ReportCyber o visitando: cyber.gov.au
- Si le preocupa que su información personal haya estado expuesta y se haya utilizado de forma indebida, póngase en contacto con el Servicio Nacional de Apoyo Cibernético e Identidad (National Identity and Cyber Support Service, IDCARE) de Australia en el teléfono 1300 432 273 o en idcare.org
- Denuncie la estafa ante la ACCC a través de la página scamwatch.gov.au/report-a-scam. Con ello ayudará a advertir a la gente sobre las estafas que circulan en la actualidad, a vigilar las tendencias y a frustrar los intentos de estafa cuando sea posible.
- Corra la voz entre sus amistades y familiares para protegerlos.

Recuerde: Siempre hay alguien que puede ayudar, ya sea el personal de cyber.gov.au o de scamwatch.gov.au, un amigo o familiar con conocimientos técnicos o incluso un club de informática de su vecinario.

Para estar al día de las últimas estafas que debe evitar, suscríbase a las alertas por correo electrónico de Scamwatch.

Tómese el tiempo de descubrir Be Connected

Be Connected es un sitio web muy completo con recursos gratuitos pensados específicamente para apoyar a las personas mayores de Australia a conectarse de forma segura a Internet y a navegar por el mundo digital con confianza. El sitio también es útil para las familias y las organizaciones comunitarias que deseen ayudar a los miembros más mayores de la comunidad a acceder a todas las ventajas que ofrece Internet.

visite beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Programa desarrollado por eSafety como parte de la iniciativa Be Connected.