Resumen presentación web

Australian Government

Be Connected
Every Australian online.

¿Puede detectar una estafa?

Ser consciente de las estafas y de cómo funcionan es un paso importante para evitarlas. Cada año, hay personas mayores de Australia que pierden millones de dólares por las estafas. A pesar de que Internet es un lugar fantástico para explorar y conectar con los demás, no siempre podemos estar seguros de que las personas son quienes dicen ser. Una vez que conozca los trucos de los estafadores, más probabilidades tendrá de detectar las estafas.

Estafas de phishing o de suplantación de identidad

Las estafas de phishing son intentos por parte de los estafadores de engañarle haciéndole creer que son de una organización de confianza o alguien que usted conoce, con el fin de que facilite información personal, como el número y contraseña de su cuenta bancaria o el número de su tarjeta de crédito.

Los mensajes de phishing están pensados para que parezcan auténticos y a menudo copian el formato utilizado por la organización a la que el estafador finge representar, incluida la marca y el logotipo. Estas estafas pueden aparecer de muchas formas, como correos electrónicos, mensajes de texto o llamadas telefónicas. Por ejemplo, puede recibir:

- un mensaje de texto de su banco pidiéndole que confirme su contraseña
- un correo electrónico de su proveedor de Internet pidiéndole que actualice sus datos
- un mensaje de texto de un familiar desde un número nuevo diciéndole que ha perdido el teléfono y que necesita que le envíe dinero urgentemente
- una llamada telefónica de su institución financiera para alertarle de una «actividad no autorizada o sospechosa en su cuenta» o de que le cerrarán la cuenta si no actualiza sus datos
- una notificación a través de Facebook de alguien que conoce recomendando un sitio web.

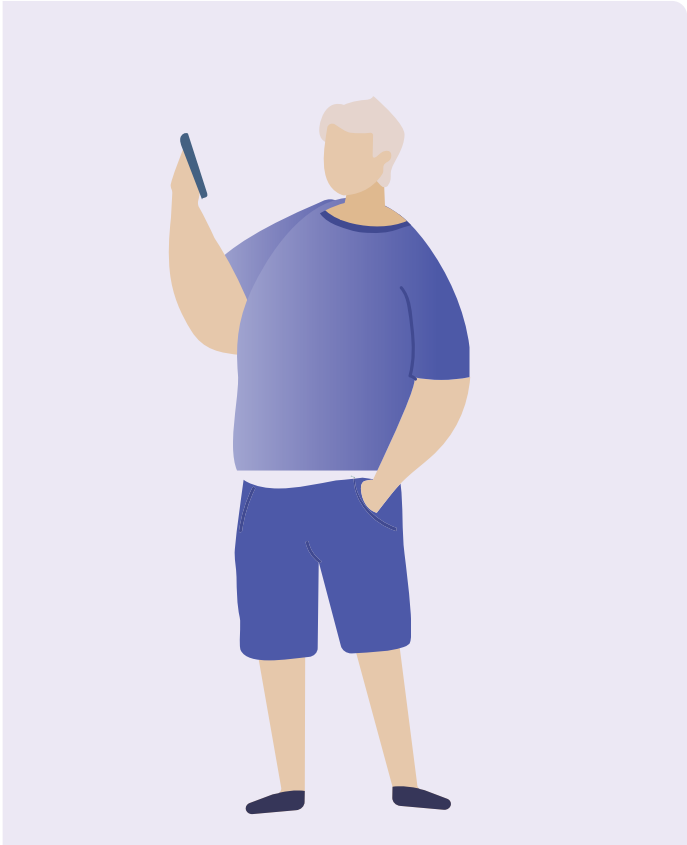
Estafas relacionadas con los impuestos y con Medicare

Los estafadores se hacen pasar por alguien de la Oficina Australiana de Impuestos (ATO), Medicare u otros organismos gubernamentales. para tratar de engañarle con el fin de que pague dinero o comparta su información personal. Estos estafadores crean sitios web falsos y envían correos electrónicos o mensajes de texto o llaman haciéndose pasar por alguien de un organismo gubernamental.

La ATO nunca le enviará correos electrónicos ni mensajes de texto ni le llamará pidiéndole que haga cosas como:

- facilitar información personal, como su número de identificación fiscal (tax file number) o los datos de su tarjeta de crédito o cuenta del banco
- pagar una tasa para recibir su devolución de impuestos o para evitar ser detenido por evasión fiscal
- hacer clic en un enlace para introducir sus datos personales
- descargar archivos o instalar programas informáticos.

Si no está seguro de si la comunicación procede de la ATO, llame a la línea directa antifraude de la ATO al 1800 008 540 o visite ato.gov.au/scams.



Cómo protegerse

- Tómeselo con calma. Vuelva a leer el mensaje. Pregúntese: ¿Es posible que el mensaje o la llamada sean falsos?
- ¿Se trata de una dirección de correo electrónico oficial o hay algo en ella que no es del todo correcto?
- ¿A quién va dirigido? Sospeche si pone «Estimado cliente» en lugar de su nombre.
- ¿Contiene errores tipográficos o gramaticales? Puede ser señal de que proviene de un estafador.
- No use lo datos de contacto que aparecen en el mensaje, ya que podrían ser falsos. Busque en Internet el número de teléfono y el sitio web oficial de la organización.
- No haga clic en ningún enlace ni abra ningún archivo adjunto, ya que podrían descargar un virus en su dispositivo.
- No dé sus datos personales, como su número de identificación fiscal (TFN), fecha de nacimiento, cuenta bancaria ni los datos de la tarjeta de crédito.

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.

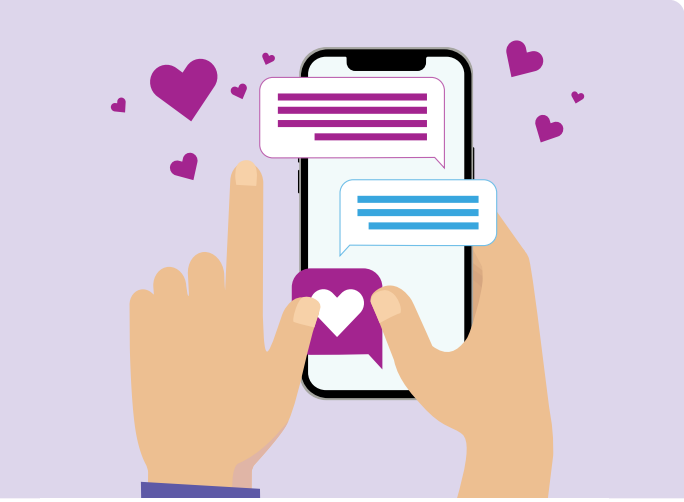
Estafas de amistad y románticas

Los estafadores se aprovechan de las personas que buscan amistad o pareja sentimental, a menudo a través de sitios web de citas, aplicaciones, redes sociales o incluso juegos de Internet, haciéndose pasar por posibles compañeros. Su objetivo es ganarse su confianza para que les envíe dinero, regalos, imágenes íntimas o les dé sus datos personales.

¿Qué puede hacer para estar alerta y no caer en la trampa?

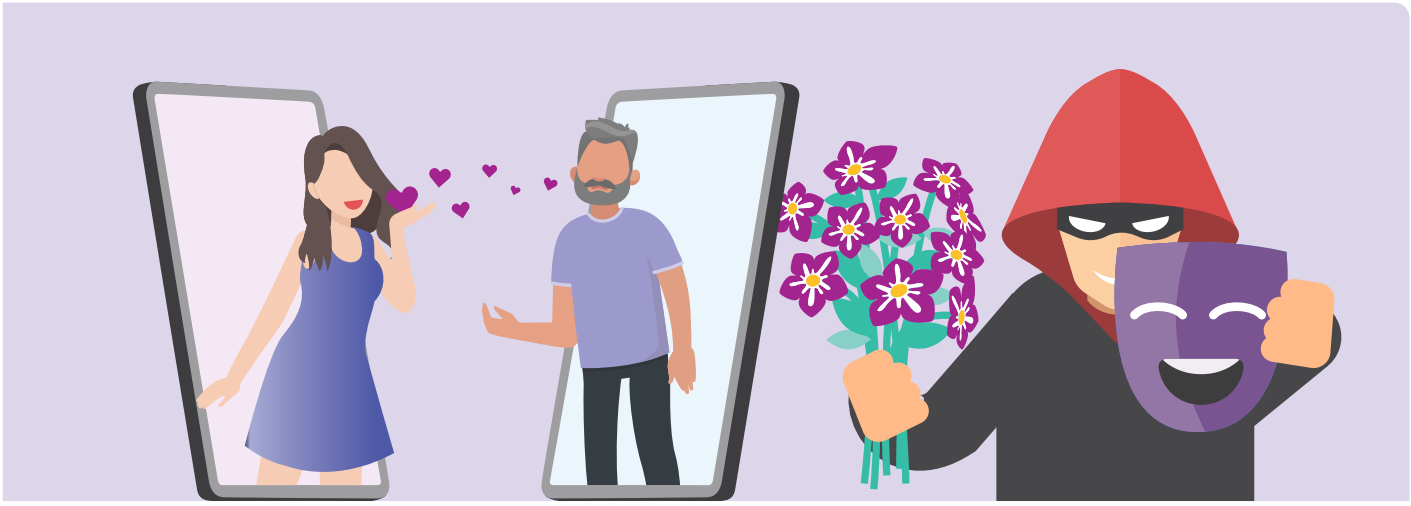
Preste atención a las personas:

- que expresen un afecto profundo por usted con mucha rapidez
- que, después de ganarse su confianza, a menudo después de esperar semanas, meses o incluso años, le cuenten una historia rebuscada y le pidan dinero o un préstamo, regalos o los datos de su cuenta bancaria o tarjeta de crédito.
- que eviten reunirse con usted en persona y pongan excusas de por qué no pueden desplazarse para ir a verle
- que tengan un perfil en línea que no es coherente con lo que cuentan sobre sí mismas.



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 en Google de las fotos de la persona en cuestión para ayudarle a determinar si realmente es quien dice ser o si las fotos están tomadas de algún otro sitio de Internet. 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 o gramaticales e incoherencias en sus relatos.
- No comparta fotos ni vídeos íntimos. Se sabe que los estafadores chantajean a sus víctimas con material comprometedor.



Estafas de soporte técnico

Estas estafas suelen comenzar con una llamada o un correo electrónico que parece proceder de una empresa grande de telecomunicaciones o informática, como Telstra, la NBN o Microsoft, indicándole que tiene un problema informático o de Internet y que ellos pueden solucionarlo. A continuación, le solicitarán acceso remoto a su computadora para «averiguar cuál es el problema» o tratarán de convencerle para que compre algún programa informático innecesario o un servicio para «solucionar» el problema.

Cómo protegerse

- Si recibe una llamada inesperada sobre su computadora y le piden acceso remoto a la misma, cuelgue.
- No facilite acceso remoto a su computadora a alguien que le hace una llamada no solicitada.
- No comparta su información personal, como los datos de su cuenta de banco o tarjeta de crédito.
- No compre programas informáticos a raíz de una llamada o un correo no solicitados.
- Ignore los mensajes emergentes que le digan que llame al soporte técnico.

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 vecindario.

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.