Cómo detectar una estafa

En Internet, no siempre podemos estar seguros de que las personas son quienes dicen ser. Ser consciente de que hay estafadores en Internet es uno de los primeros pasos para evitarlos. Una vez que conozca sus timos, debería ser más fácil detectar un fraude cuando lo vea.

Mensajes de correo electrónico fraudulentos

Los mensajes fraudulentos (phishing) son el tipo de fraude más común de Internet. Pueden parecer que provienen de una organización fiable, pero están diseñados para engañarle para que dé sus datos personales como la cuenta bancaria, el número de tarjeta de crédito, su usuario y sus contraseñas.

Pueden aparecer de muchas maneras:

- correos electrónicos inesperados, mensajes de texto o llamadas telefónicas que le piden que confirme, actualice o ingrese de nuevo sus datos personales
- mensajes urgentes o amenazantes diciéndole que pasa algo inusual con su cuenta o que su cuenta se va a cerrar, así que tiene que hacer clic en un enlace para resolver la situación
- correos inesperados le piden que abra o descargue un archivo ".exe" o ".zip".

Consejo: si no está seguro del mensaje que ha recibido, busque en Internet la empresa que parece que lo ha enviado y póngase en contacto con ellos directamente.

Vaya despacio. Vuelva a leer el mensaje.

- ¿Quién lo envía? ¿Es una dirección oficial de correo electrónico o una que parece extraña?
- ¿A quién va dirigido? Sospeche si se trata de "Estimado cliente" en lugar de su nombre.
- ¿Tiene errores de ortografía y gramática? Esto puede ser un signo de que proviene de un estafador.

Qué no hacer:

- hacer clic en ningún enlace
- abrir ningún archivo adjunto, ya que puede descargar un virus informático
- utilizar los datos de contacto que se facilitan en el mensaje, podrían ser falsos.

Fraudes sobre impuestos y Medicare

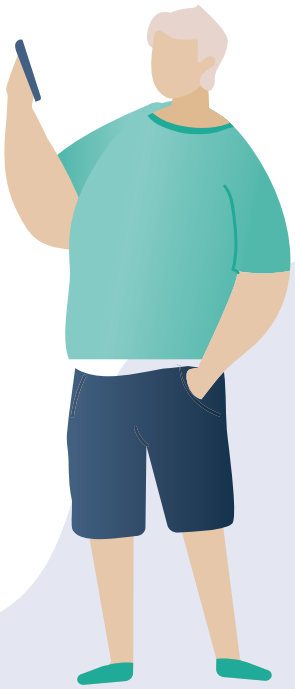
Los estafadores se hacen pasar por la Australian Taxation Office (Oficina Australiana de Impuestos), Medicare y otras organizaciones gubernamentales para conseguir dinero y la información personal de las víctimas a través de llamadas, mensajes de texto, correos electrónicos y páginas web falsas.

Es importante recordar que la Australian Tax Office (ATO) nunca:

- le enviará un correo ni un mensaje de texto pidiéndole su información personal, incluyendo su TFN, su tarjeta de crédito o los datos bancarios
- le pedirá que pague una tasa para recibir su devolución de impuestos o para que no le arresten por evadir impuestos
- le enviará un correo electrónico con un enlace a un servicio en línea que le pida sus datos personales
- le enviará archivos para descargar ni le pedirá que instale un software.

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

- No haga clic en ningún enlace ni descargue ningún archivo adjunto.
- No dé sus datos personales como su número de contribuyente (TFN), la fecha de nacimiento, la cuenta bancaria ni los datos de la tarjeta de crédito.
- No utilice los datos de contacto facilitados si no está seguro de si un mensaje telefónico es real, en su lugar busque en Internet el número de la organización.
- Conocer el estado de sus asuntos fiscales: ¿es probable que le tengan que pagar una devolución de impuestos o que tenga un pago pendiente?
- Inicie sesión en su cuenta oficial de myGov escribiendo manualmente la dirección en lugar de hacer clic en un enlace.
- Compruebe si el correo electrónico que ha recibido es de la dirección real de ATO, que acaba en @ato.gov.au
- Incluso si parece que está en el sitio web de la ATO o en myGov, compruebe que la dirección acaba en ".gov.au" (en lugar de en ".com.au", ".org.au" o ".net.au", por ejemplo).
- Buscar errores de ortografía y gramática
- Sospeche de mensajes que no se dirijan directamente a usted.



Fraudes sobre citas y buscar pareja

Los estafadores crean perfiles falsos en línea en las redes sociales o en sitios de citas para ponerse en contacto con sus víctimas. Su objetivo es ganarse su confianza antes de pedirle dinero.

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

Estar atento a:

- personas que le expresan mucho afecto muy rápidamente antes de pedirle dinero o un "préstamo"
- personas que eviten encontrarse cara a cara y que pongan excusas como que no pueden viajar para verle
- personas cuyos perfiles en línea no coincidan con lo que han dicho sobre ellas mismas.

Qué hacer:

- comprobar si sus imágenes son realmente de ellos o si las tomado de otra persona en Internet haciendo una búsqueda de imágenes en Google. Ir a images.google.com y hacer clic en el icono de la cámara
- sospeche cuando comiencen a mencionar problemas de dinero o que necesitan dinero para una "emergencia"

Qué no hacer:

- transferir dinero a alguien con quien solo ha hablado por teléfono o por correo electrónico
- enviar información personal como su fecha de nacimiento, los datos bancarios o de la tarjeta de crédito.

Estafas de soporte técnico

Estas estafas normalmente comienzan con una llamada o un correo electrónico, que parecen ser de una empresa grande y muy conocida, indicándole que tiene un problema en la computadora o en Internet y que ellos pueden solucionarlo.

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

- No facilitar acceso remoto a su computadora.
- No darles información personal como su cuenta bancaria o los datos de su tarjeta de crédito.
- No comprar software a partir de una llamada o un correo no solicitados.
- Ignorar los mensajes emergentes que le digan que llame al soporte técnico.

Las empresas grandes esperan que usted les llame cuando tiene un problema con Internet o su computadora. Ellos no le llamarán.

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 y detenga cualquier otro pago hacia el estafador
- reporte el fraude a la Australian Competition and Consumer Commission (Comisión Australiana de Competición y Consumidores) en scamwatch.gov.au, ellos pueden ayudarle con más consejos
- ayude a concienciar a otras personas. Si alguien que conoce puede también ser víctima del fraude, avíselo.

Si no está seguro de si un mensaje que ha recibido proviene realmente de la ATO o si ha sido víctima de un fraude relacionado con impuestos, llame al **servicio telefónico de fraudes de la ATO** en el teléfono **1800 008 540**.

Manténgase informado sobre los fraudes de ATO visitando ato.gov.au/scams

Si le preocupa que su información personal se haya visto expuesta o se la hayan usurpado, póngase en contacto con Australia's National Identity and Cyber Support Service **IDCARE** (Servicio de Identidad Nacional y Soporte Cibernético de Australia, IDCARE) en el teléfono **1300 432 273** o en idcare.org

Recuerde:

Siempre habrá alguien que pueda ayudar: los chicos de scamwatch.gov.au, un amigo o familiar al que se le den bien las computadoras o incluso un club local de informática.

Los fraudes están pensados para aprovecharse de su buena disposición, pero Internet puede ser un lugar seguro para explorar si tiene cuidado al compartir su información personal en Internet, usa el sentido común cuando decide a quién le envía dinero y no baja la guardia.

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