Los 10 mejores consejos para protegerte contra las

Estafas de suplantación de identidad

Spanish | Español

Australian Government | Be Connected Every Australian online.

Australian Government | National Anti-Scam Centre | SCAMWATCH

Las estafas de hoy en día son cada vez más sofisticadas. Antes, la mala ortografía y gramática las hacían fáciles de detectar, pero la nueva tecnología significa que las estafas son cada vez más difíciles de detectar.

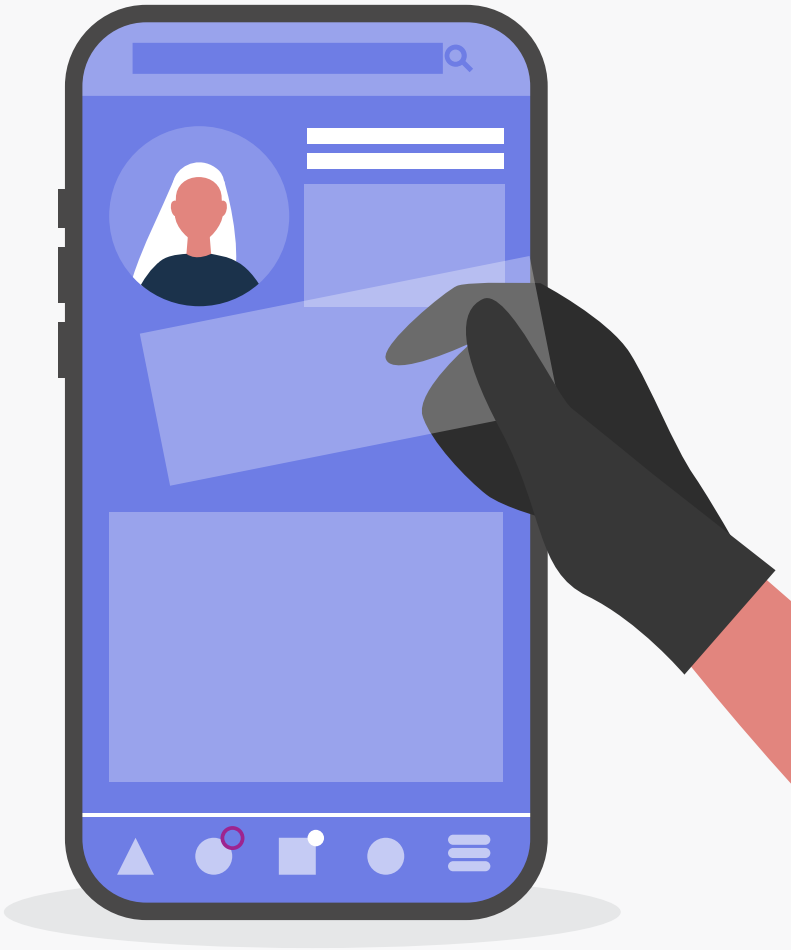
El Centro Nacional de Protección Contra Estafas se ha unido al Gobierno, expertos del sector, organismos de aplicación de la ley y organizaciones comunitarias para combatir las estafas. Sin embargo; también hay pasos que tú puedes seguir para evitar que te estafen. Una de las mejores medidas de protección es mantenerse al día con las nuevas estafas emergentes para que puedas reconocer las señales.

Be Connected se ha asociado con Scamwatch, del Centro Nacional de Protección contra Estafas, para traerte esta guía que te ayudará a detectar estafas de suplantación, protegerte contra ellas y saber adónde acudir en caso de que alguna vez resultes víctima de una estafa.

Todos los ejemplos proporcionados en esta guía son estafas reales.

En esta guía

- ¿Qué es una estafa de suplantación?
- ¿Qué es el "spoofing"?
- Estafas comunes de suplantación
- Los 10 mejores consejos para protegerte
- ¿Adónde acudir para obtener ayuda?



¿Qué es una estafa de suplantación?

Las estafas de suplantación están diseñadas para parecer que provienen de organizaciones legítimas que conoces. Pueden parecer que son de tu banco, proveedor de servicios de internet, una agencia gubernamental, vendedor, o incluso un estafador que finge ser un amigo o familiar.

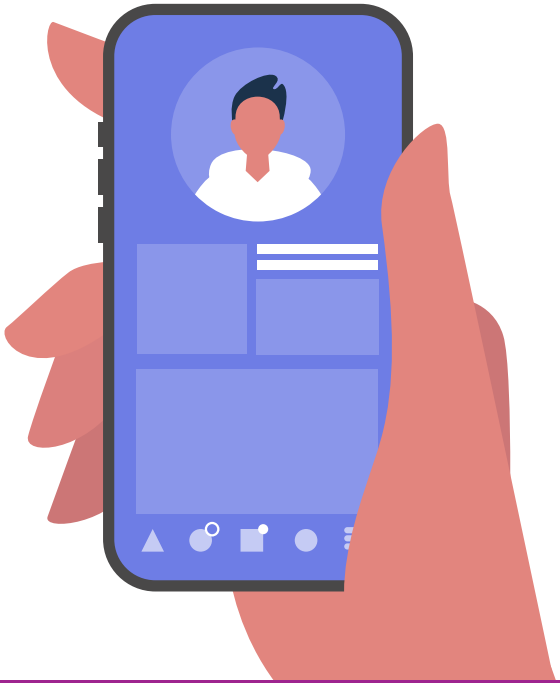
Al pretender venir de alguien en quien confías, los estafadores utilizan un sentido de urgencia para engañarte y hacerte pagar dinero o proporcionar información personal, como contraseñas importantes, datos de tarjeta de crédito o bancarios.

Los estafadores utilizan una variedad de métodos para ponerse en contacto contigo, incluidos mensajes de texto, llamadas telefónicas, correos electrónicos, publicaciones en redes sociales y sitios web falsos que se ven idénticos a los sitios web oficiales.

¿Qué es el "spoofing"?

Los estafadores pueden hacerse pasar por organizaciones conocidas utilizando tecnología que hace que sus llamadas o mensajes parezcan provenir de una fuente confiable. A esto se le conoce como "spoofing".

Mantente alerta ante las estafas y cuestiona el contacto no solicitado que pida información personal, como una contraseña o algún tipo de pago. Contacta directamente a la organización a la que dicen pertenecer para confirmar.



Existen diferentes tipos de técnicas de "spoofing", entre las que se incluye:

01. **Suplantación de ID de llamada:** los estafadores alteran su ID de llamada para mostrar un número de teléfono diferente al que se está utilizando, haciendo que la llamada parezca provenir de un número legítimo.

02. **Suplantación de SMS (o etiquetas alfa):** los estafadores alteran su número de teléfono para que aparezca como el nombre de una empresa (por ejemplo, AusPost). Pueden hacer que un mensaje de texto aparezca en la misma conversación o hilo de mensajes genuinos de una organización.

03. **Suplantación de correo electrónico:** los estafadores alteran su dirección de correo electrónico o nombre del remitente para hacer que un correo electrónico parezca provenir de una fuente confiable. Pueden falsificar el nombre que aparece en "De" o la dirección de correo electrónico, a menudo cambiando o agregando una letra o número a un nombre de dominio legítimo (por ejemplo, @amaz0n.com en lugar de @amazon.com).

Estafas habituales de suplantación de identidad

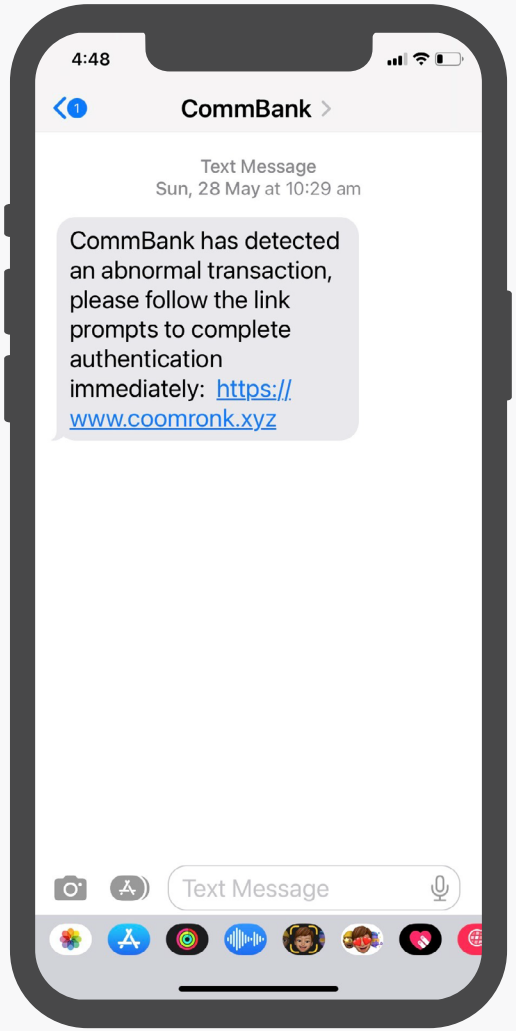
Estafas de suplantación bancaria

- Recibes una llamada o un mensaje de texto de alguien que dice ser del departamento de seguridad de tu banco. La persona te informa acerca de una transacción sospechosa, y afirma que tu cuenta se encuentra en riesgo. Te insta a transferir dinero a otra cuenta para "mantenerlo seguro" o para "una investigación adicional".
- Recibes un mensaje de texto o un correo electrónico pidiéndote que hagas clic en un enlace para verificar los datos de tu cuenta. El enlace te lleva a un sitio web falso diseñado para obtener tu nombre de usuario, contraseña y otra información personal.

¿Cómo saber si es una estafa?

Si bien tu banco puede contactarte si hay actividad sospechosa en tu cuenta, nunca te pedirá que transfieras fondos a otra cuenta. Tampoco te pedirá información sobre ninguna cuenta o datos personales, incluyendo tu contraseña, PIN o código de un solo uso en un mensaje de texto, correo electrónico o llamada telefónica no solicitada.

Los estafadores pueden hacer que un número de teléfono se parezca al identificador de llamada de tu banco, pero no tomes eso como prueba de con quién estás hablando. También pueden parecer tener información sobre ti, pero es probable que cualquier dato que tengan haya sido obtenido fraudulentamente.



Ejemplo de un mensaje de texto de suplantación de identidad de un número falsificado pidiéndote que hagas clic en un enlace para verificar tus datos.

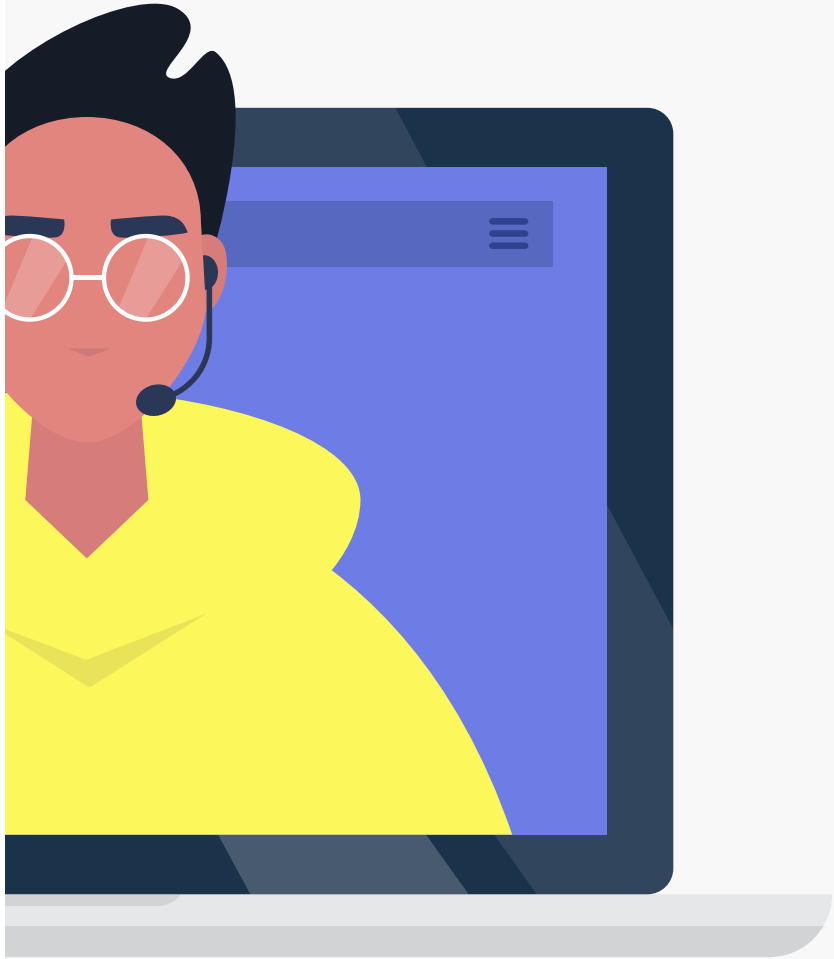
Estafas de soporte técnico

- Una persona que llama y dice trabajar para un proveedor de servicios de internet, telecomunicaciones o empresa de computación te informa que hay un problema con tu internet o computadora. Te pueden decir que ha sido hackeada, tiene un virus, está funcionando lentamente o está a punto de desconectarse. Te dan instrucciones para que descargues una aplicación o software para darles acceso remoto a tu computadora para que puedan "arreglarla".
- Un mensaje de advertencia aparece en la pantalla de tu computadora instándote a llamar inmediatamente al número de teléfono listado para obtener ayuda con un problema que ha sido detectado.

¿Cómo saber si es una estafa?

Las empresas legítimas nunca llamarán para decirte que hay un problema con tu conexión a internet o computadora (esperan que seas tú quien las contacte en caso de un problema). Nunca te pedirán que descargues ningún tipo de software o aplicación que les dé acceso a tu dispositivo.

Cierra los mensajes emergentes sospechosos haciendo clic en la "x" en la esquina superior derecha de la caja. Si eso no funciona, intenta hacer clic fuera de la caja o cierra la página web en la que aparece. Si el mensaje emergente aún no ha desaparecido, prueba mantener presionadas las teclas ALT y F4 en computadoras Windows para cerrar el navegador web. En una computadora Apple, selecciona "Forzar salida" en el menú de Apple y selecciona el navegador que deseas cerrar.



Estafas de suspensión de cuenta

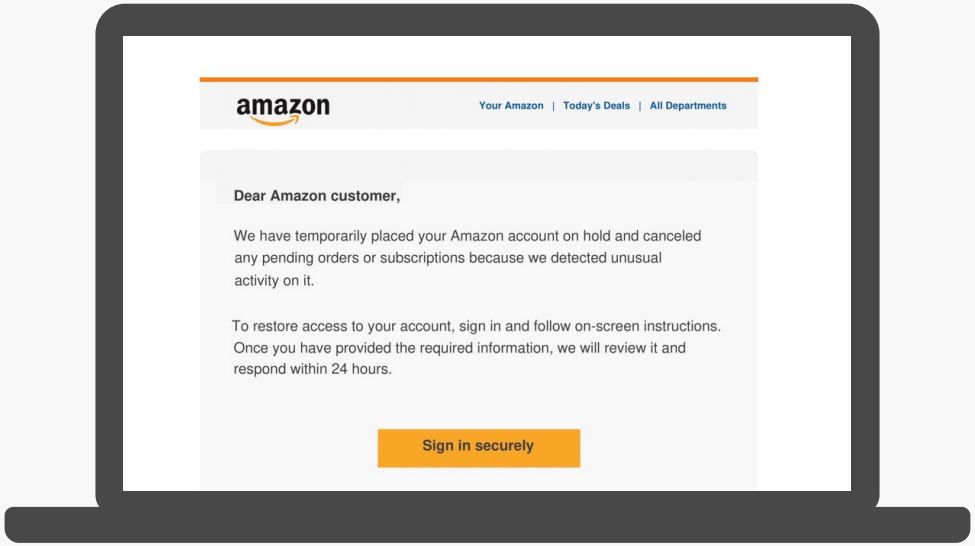
Recibes un correo electrónico o un mensaje de texto que dice ser de una organización que conoces, como Amazon, PayPal o Netflix. Te informan que tu cuenta ha sido suspendida debido a actividad sospechosa y que necesitas hacer clic en un enlace para confirmar tu identidad y sepan que realmente eres tú.

Los estafadores utilizan tácticas de miedo para dirigirte a un sitio web falso que captura datos personales como tu nombre de usuario, contraseña y datos bancarios o de tarjeta de crédito.

¿Cómo saber si es una estafa?

Amazon, PayPal y Netflix nunca pedirán información personal como tus contraseñas, datos bancarios o de tarjeta de crédito a través de un enlace en un correo electrónico o mensaje de texto no solicitado. Mientras que las organizaciones difieren en su enfoque para contactar a los clientes, es mejor ser precavido/a y siempre tratar estos tipos de correos electrónicos, mensajes de texto o llamadas con cautela.

Si tienes dudas acerca de si un mensaje es realmente de la empresa que dice ser, contáctalos directamente buscando sus datos de contacto en línea. Nunca uses los datos de contacto proporcionados en el texto, correo electrónico o llamada telefónica.



Ejemplo de un correo electrónico de estafa que afirma ser de Amazon instándote a hacer clic en el enlace para proporcionar tu información personal.

Ten cuidado con las tácticas de miedo

Los estafadores utilizan tácticas de miedo para crear un sentido de urgencia y hacer que actúes. Aquí hay algunas cosas que pueden decir para captar tu atención:

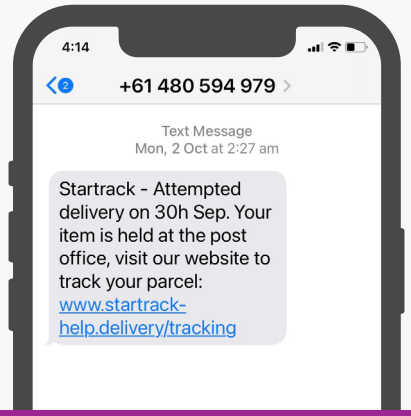
- Se ha detectado actividad inusual en la cuenta
- Intentos de inicio de sesión no autorizados
- Tu cuenta está bloqueada / cerrada
- Tu pago fue rechazado
- No podemos validar tu información de facturación

Estafas de intento de entrega fallido

Recibes un correo electrónico o mensaje de texto que afirma ser de Australia Post o una empresa de mensajería como FedEx informándote que hay un problema o retraso con tu entrega. Para recibir tu paquete, necesitarás pagar un costo de envío o "actualizar tus datos".

¿Cómo saber si es una estafa?

Australia Post, FedEx y otras empresas de mensajería legítimas nunca enviarán un mensaje de texto, correo electrónico o llamarán para pedir información personal o pagos. Si esperas una entrega, lo mejor es rastrearla través de la aplicación segura o mediante el servicio de seguimiento en línea en el correo electrónico de confirmación de tu pedido. Si no tienes uno, llama directamente a la empresa de mensajería para preguntar sobre el estado de tu paquete.



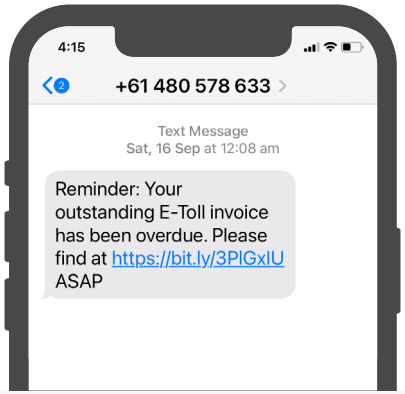
Ejemplo de un mensaje de texto que afirma ser de una empresa de mensajería.

Estafas de peajes

Recibes un mensaje de texto de un operador de peaje informándote que tu pago de peaje está atrasado. Necesitas tomar medidas inmediatas para evitar pagar una multa, por lo que incluyen un enlace para que organices el pago, pero te lleva a un sitio web falso diseñado para robar tus datos financieros.

¿Cómo saber si es una estafa?

Si has recibido un mensaje de texto que afirma que tienes una cuenta de peaje vencida o fondos insuficientes, podría ser una estafa. Visita el sitio web o la aplicación del operador de peaje para iniciar sesión en tu cuenta y verificar tu actividad reciente.



Ejemplo de un mensaje de texto de estafa de peaje.

Estafas de inversiones falsas

Ves una increíble oportunidad de inversión que parece estar respaldada por una celebridad o un influencer de finanzas. Promete la garantía de grandes ganancias con poco o ningún riesgo. Cuando preguntas, te dirigen a un sitio web de aspecto profesional y recibes material promocional sofisticado.

¿Cómo saber si es una estafa?

Si una oferta suena demasiado buena para ser verdad, lo más probable es que sea una estafa. Los estafadores utilizan tácticas de alta presión para convencerte de actuar rápidamente para que no "te pierdas" algo. Cuidado con correos electrónicos, sitios web o anuncios con testimonios y promesas exageradas de grandes ganancias.

El "asesor" que te está ayudando puede afirmar que no necesita una licencia de servicios financieros australianos (AFS). Si te proporcionan una, siempre verifica que la persona con la que estás tratando sea el verdadero titular de la licencia.

Estafas de sitios web falsos

Ves un anuncio en Facebook de una conocida marca de asadores que se vende por $100 cuando normalmente cuesta $900. Haces clic en el enlace al sitio del minorista y ves que los pagos con tarjeta de crédito tienen una tarifa del 2.99 %, así que optas por pagar mediante transferencia bancaria directa para recibir un descuento adicional del 5 %. Recibes un correo de confirmación pero nunca te llega el asador.

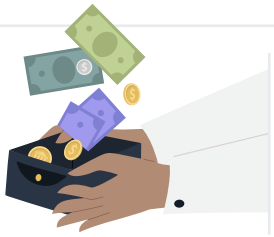
¿Cómo saber si es una estafa?

Los sitios web falsos tienen precios que son demasiado buenos para ser verdad, formas de pago inusuales y otras señales de advertencia, como una URL que intenta parecerse a la URL de una tienda oficial (por ejemplo, webberbbqs.com en lugar de la verdadera weber.com).

Los estafadores también pueden pagar anuncios en redes sociales y motores de búsqueda como Google (conocidos como anuncios patrocinados), así que ten cuidado al hacer clic en este tipo de anuncios.

Los 10 mejores consejos para protegerte

01. Cuidado con las llamadas no solicitadas. Deja que las llamadas de números de teléfono que no reconoces se vayan al buzón de voz.



02. Detente y piensa antes de proporcionar datos personales o financieros a través de comunicaciones no solicitadas. Pregúntate: ¿podría ser falso?

03. Cuidado con los correos electrónicos que utilizan tácticas de miedo. Compara el nombre que aparece y la dirección de correo electrónico. ¿Coinciden? Por ejemplo, el campo "De" dice "Soporte de Amazon" pero la dirección de correo electrónico es "amazonsupport830@gmail.com"

04. No confíes en un mensaje de texto solo porque aparece en el mismo hilo que otros mensajes de una organización que conoces; aún así podría tratarse de una estafa.

05. Si tienes dudas sobre un mensaje o llamada que hayas recibido, contacta a la organización que dicen ser. Contáctalos a través de su sitio web oficial o aplicación segura en tu teléfono inteligente o tableta.

06. Nunca proporciones tu contraseña, PIN o código de un solo uso a nadie por teléfono, incluso si afirman ser de tu banco o de una agencia gubernamental y te leen información sobre tu cuenta.

07. Nunca hagas clic en enlaces recibidos por mensaje de texto. Si bien es posible que algunos sean inofensivos, es mejor tener precaución. Lo mismo ocurre con los archivos adjuntos y enlaces en correos electrónicos, a menos que confíes en el remitente.

08. Nunca sigas las instrucciones de una llamada no solicitada si la persona que llama te pide que descargues una aplicación o instales un software que le permita acceder a tu dispositivo. Cuelga de inmediato.

09. Nunca inicies sesión en tus cuentas en línea a través de un enlace en un correo electrónico o mensaje de texto. En vez de esto, ingresa la URL en tu navegador web o utiliza la aplicación segura de la empresa para acceder a tu cuenta.

10. Antes de realizar un pago en línea, siempre verifica la URL del sitio web (¿es el sitio oficial?), identifica si los métodos de pago son inusuales, la información está mal redactada o si falta información en las secciones "Acerca de nosotros", "Envíos y Devoluciones" y otras secciones que se encuentran en la parte inferior del sitio web.

Si alguna vez tienes dudas, haz una búsqueda en línea ingresando el nombre de la organización o el sitio web en cuestión y la palabra "estafa".

¿Crees que te han estafado?

¿Adónde ir para obtener ayuda?

Ser estafado/a puede tener un costo financiero y emocional, por lo que es importante buscar ayuda y actuar rápidamente. Hay varios pasos que puedes seguir:

1. Contacta a tu banco de inmediato para detener cualquier transacción adicional.
2. Contacta a IDCARE, un servicio de apoyo gratuito para personas que han sido afectadas por estafas o robo de identidad. Llama 1800 595 160 o visita idcare.org
3. Cambia tus contraseñas de inmediato y asegúrate de que sean seguras.
4. Informa sobre la estafa a Scamwatch para advertir a otros: scamwatch.gov.au/report-a-scam
5. Busca apoyo. Si no te sientes cómodo/a hablando con amigos o familiares, contacta a Lifeline o Beyond Blue para una charla confidencial. Y si has perdido una cantidad significativa de dinero, habla con la Línea Nacional para la Deuda (National Debt Helpline).

   Beyond Blue: 1300 22 4636 (24/7) o visita beyondblue.org.au

   Lifeline: 13 11 14 (24/7) o visita lifeline.org.au

   Línea Nacional de Asistencia sobre Deudas: 1800 007 007 (de lunes a viernes de 9:30 a.m. a 4:30 p.m.) o visita ndh.org.au

Para más información

Haz clic en los recuadros de abajo para explorar:

PODCAST

Cómo evitar estafas de suplantación

PODCAST

Lo que los estafadores en línea no quieren que sepas

TEMA

Identificar y evitar estafas

TEMA

Seguridad en línea avanzada

ARTÍCULO

Cómo parar las llamadas no deseadas

ARTÍCULO

Robo de identidad: ¿qué es y cómo evitarlo?

El Pequeño Libro de las Estafas es una herramienta reconocida internacionalmente que te ayuda a aprender más sobre una variedad de estafas comunes y cómo puedes protegerte contra ellas.

Visita el sitio web de Scamwatch para mantenerte al día con las últimas estafas y consejos sobre cómo protegerte contra ellas.

Australian Government | Be Connected
Every Australian online.

Acerca de Be Connected

Be Connected es una iniciativa del Gobierno australiano comprometida a desarrollar las habilidades digitales, la confianza y la seguridad en línea de los australianos mayores con clases de computación gratuitas, cursos cortos en línea y mucho más sobre una variedad de temas. El sitio web de Be Connected y el contenido de aprendizaje son gestionados por el Comisionado de eSafety.

Australian Government | National Anti-Scam Centre | SCAMWATCH

Acerca de Scamwatch

Scamwatch es administrado por el Centro Nacional de Protección contra Estafas, el cual fue creado para hacer de Australia un objetivo más difícil para los estafadores. Aumenta la conciencia sobre las estafas educando a la comunidad sobre cómo reconocer, evitar y denunciar estafas. El Centro de Protección contra Estafas comparte información de denuncias de estafas y trabaja con el Gobierno, organismos de aplicación de la ley y el sector privado para interrumpir y prevenir estafas.