Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

LA CIBERSEGURIDAD PERSONAL

PRIMEROS PASOS

cyber.gov.au

Serie sobre la ciberseguridad personal

Serie sobre la ciberseguridad personal

La guía de ***Ciberseguridad personal: Primeros pasos*** es la primera de una serie de tres guías producidas para facilitarles a los australianos la comprensión de los fundamentos de la ciberseguridad. Aprenda a tomar medidas para protegerse de los peligros cibernéticos comunes.

Primeros pasos

Próximos pasos

Pasos avanzados

Índice

Introducción

¿Qué es la ciberseguridad personal?

En un mundo cada vez más tecnificado, todos los días usamos dispositivos y cuentas que son vulnerables a los peligros cibernéticos:

- Sus dispositivos pueden incluir computadoras (ordenadores), teléfonos celulares, tabletas y otros dispositivos conectados a internet.
- Posiblemente también utilice cuentas en línea para correo electrónico, transacciones bancarias, compras, medios sociales, juegos y mucho más.

La ciberseguridad personal consiste en los pasos constantes que puede dar para proteger sus cuentas y dispositivos de los peligros cibernéticos.

¿En qué puede ayudar esta guía para protegerme de los peligros cibernéticos?

Si ésta es la primera vez que está aprendiendo acerca de la ciberseguridad, o si se está manteniendo al día, esta guía es un punto de partida excelente. La guía «La ciberseguridad personal: primeros pasos" es la primera de una serie de tres guías formuladas para facilitar la comprensión de los fundamentos de la ciberseguridad.

¿Qué son los peligros cibernéticos?

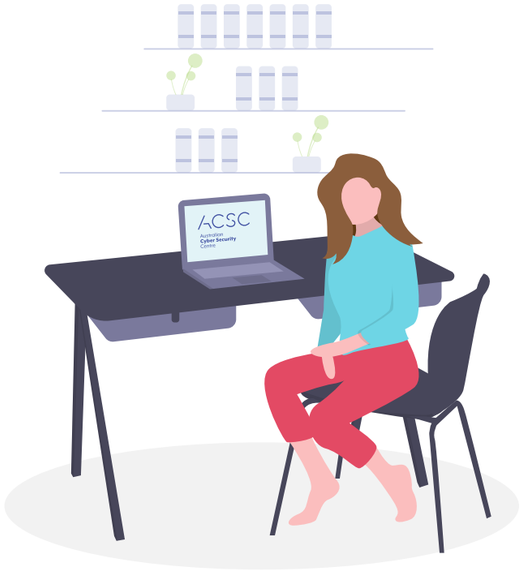
Los principales peligros cibernéticos que afectan a los australianos son **las estafas y el malware o software malicioso**.

- **"Malware" es un término general usado para describir el software malicioso** creado para causar daño. Puede incluir los virus, gusanos informáticos, spyware, troyanos y ransomware.

Los ciberdelincuentes usan el software malicioso para robar información y dinero, y para controlar cuentas y dispositivos ajenos.

- **Scams son mensajes enviados por ciberdelincuentes** con el objeto de manipularle a usted para que entregue información confidencial o active malware en su dispositivo.

Estos ataques pueden tener consecuencias personales y financieras significativas para las víctimas. También están aumentando en complejidad y frecuencia.



Active las actualizaciones automáticas

¿Qué son las actualizaciones?

La actualización es una versión mejorada del software (programas, aplicaciones y sistemas operativos) que tiene instalados en su computadora y dispositivos móviles.

- **Las actualizaciones del software ayudan a proteger sus dispositivos** al arreglar los errores de codificación o vulnerabilidades del software. Los ciberdelincuentes y el software malicioso pueden usar estos "errores" para acceder a su dispositivo y robar sus datos personales, cuentas, información financiera e identidad.
- **Los ciberdelincuentes descubren y utilizan constantemente nuevos errores de software**. La actualización del software cargado en sus dispositivos ayuda a protegerle de los ciberataques.

¿Cómo configuro actualizaciones automáticas?

Las actualizaciones automáticas son una selección predeterminada o "fijada y olvidada" que instala nuevas actualizaciones tan pronto como están disponibles.

- **Active y confirme las actualizaciones automáticas** de todo el software y en todos los dispositivos.
- **El método de activación de las actualizaciones automáticas puede ser diferente** según el software y dispositivo.
- Si es posible, **elija un horario conveniente para las actualizaciones automáticas**, por ejemplo cuando está durmiendo o no está usando su dispositivo.

El dispositivo debe estar encendido, enchufado a la electricidad y tener espacio de almacenamiento no utilizado.

Sugerencia: Si recibe un mensaje recordatorio de actualizar el software de su dispositivo, hágalo lo más rápidamente posible.

Para obtener información más detallada sobre cómo activar las actualizaciones automáticas busque "Updates" en cyber.gov.au

¿Qué debo hacer si no hay una selección para actualizaciones automáticas?

Si no hay una selección para actualizaciones automáticas, compruebe periódicamente si hay nuevas actualizaciones e instálelas por medio del menú de selecciones de su software o dispositivo.

¿Qué debo hacer si mi dispositivo y software más antiguos no reciben actualizaciones?

Si su dispositivo, sistema operativo o software son viejos, es posible que ya no reciban asistencia del fabricante o diseñador.

Cuando los productos llegan a esta etapa de "fin de la asistencia", ya no reciben actualizaciones. Esto puede dejarle a usted a la merced de ciberataques. Ejemplos de productos que han llegado al final de la asistencia: sistema operativo Windows 7 y el iPhone 7.

Si su dispositivo, sistema operativo o software han llegado al final de la asistencia, el ACSC (Centro australiano de ciberseguridad) aconseja actualizarlo cuanto antes para mantenerse seguro.

Para obtener más información, busque "End of support" en cyber.gov.au

Active la autenticación multifactorial (MFA).

¿Qué es la MFA?

Puede utilizar la autenticación multifactorial (MFA) para mejorar la seguridad de sus cuentas más importantes. La MFA requiere una combinación de dos o más tipos de autenticación antes de permitir el acceso a una cuenta.

- **Algo que usted conoce** (p.ej. un PIN, contraseña o frase de contraseña)
- **Algo que usted tiene** (p.ej. una tarjeta inteligente, un testigo físico, una aplicación de autenticación, un SMS o e-mail)
- **Algo que usted es** (p.ej. una huella digital, reconocimiento facial o escaneo del iris)

Con la MFA los ciberdelincuentes tienen más dificultades para conseguir acceso a sus cuentas. La MFA añade más capas de autenticación, y penetrarlas exige más tiempo, esfuerzo y recursos.

¿Cómo puedo activar la MFA para proteger mis cuentas más importantes?

Los pasos de la activación de la MFA son diferentes según la cuenta, el dispositivo o aplicación de software. Active la MFA ahora mismo, empezando por sus cuentas más importantes:

- Todas las cuentas de transacciones bancarias y financieras en línea (p.ej. su banco, PayPal)
- Todas las cuentas de correo electrónico (p.ej. Gmail, Outlook, Hotmail, Yahoo!)

Si tiene muchas cuentas de correo electrónico, priorice las que estén vinculadas con sus transacciones bancarias en línea u otros servicios importantes.

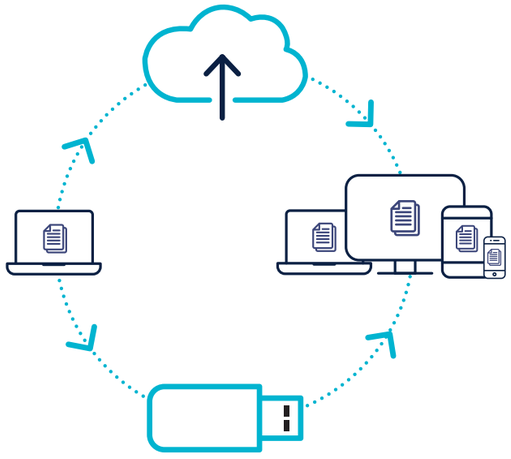
Para leer más sobre cómo activar la autenticación multifactorial busque "Multi-factor authentication" o "MFA" en cyber.gov.au

Guarde copias de seguridad de sus dispositivos regularmente.

¿Qué es una copia de seguridad?

Las copias de seguridad son copias digitales de su información. Esto puede incluir cosas como fotos, información financiera o registros que ha guardado en un dispositivo de almacenamiento externo, o en la nube.

Las copias de seguridad de su información son una medida cautelar que le permitirá recuperarla si alguna vez se pierde, se la roban o se daña.



¿Cómo hago copias de seguridad de mis dispositivos y archivos?

Debe hacer copias de seguridad de sus archivos y dispositivos regularmente. Usted decide cómo lo hace, si es a diario, semanal o mensualmente.

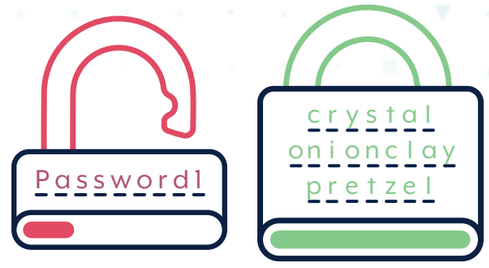
El número de veces que haga copias de seguridad dependerá del número de:

- archivos nuevos que cargue en su dispositivo,
- cambios que haga a sus archivos.

Sugerencia: Compruebe regularmente sus copias de seguridad para conocer bien el proceso de recuperación. Asegúrese siempre de que sus copias de seguridad funcionan bien.

Encontrará información más detallada sobre cómo hacer copias de seguridad de su información bajo “Backups” en cyber.gov.au

Use frases de contraseña para proteger sus cuentas importantes



La autenticación multifactorial (MFA) es una de las formas más eficaces de proteger sus cuentas contra los ciberdelincuentes. **Si la MFA no está disponible**, una frase de contraseña única y resistente puede proteger mejor su cuenta que una contraseña simple.

¿Qué es una frase de contraseña?

Las frases de contraseña utilizan cuatro o más palabras al azar como contraseña.

Por ejemplo: “cristal cebolla arcilla pretzel”.

- **Las frases de contraseña son más seguras** que las contraseñas simples.
- **Los ciberdelincuentes tienen dificultades** en adivinar las frases de contraseña, pero **usted las recordará fácilmente**.

¿Cómo hago para crear una frase de contraseña?

Cree frases de contraseña que sean:

- **Largas:** de un mínimo de 14 caracteres, y que usen cuatro o más palabras al azar. Cuanto más larga la frase de contraseña, más segura será.
- **Imprevisibles:** use una mezcla al azar de cuatro o más palabras que no estén relacionadas. No use frases famosas, citas o la letra de una canción.
- **Únicas:** no vuelva a usarlas en más de una cuenta.

Si una página web o servicio requiere una contraseña compleja que incluya símbolos, mayúsculas o números, usted puede incluirlos en su frase de contraseña. De todos modos, su frase de contraseña deberá ser larga, imprevisible y única para que sea lo más segura posible.

¿Qué cuentas debo proteger con una frase de contraseña?

Si sus cuentas más importantes no están protegidas por MFA, cambie sus contraseñas por frases de contraseña únicas y fuertes; comience por:

- Las cuentas de transacciones bancarias y financieras en línea
- Las cuentas de correo electrónico

Si tiene muchas cuentas de correo electrónico, priorice las que estén vinculadas con sus transacciones bancarias u otros servicios importantes en línea.

También puede cambiar su contraseña por una frase de contraseña única y fuerte mediante el menú de selecciones de su cuenta.

Sugerencia: Si le cuesta recordar todas sus frases de contraseña, piense en utilizar un gerente de contraseñas. Con un gerente de contraseñas, solo tendrá que recordar una contraseña y el gerente de contraseñas se ocupará del resto. Busque “password manager” en cyber.gov.au para obtener más asesoramiento.

Encontrará información más detallada sobre cómo crear frases de contraseña seguras bajo “Passphrases” en cyber.gov.au

Proteja su dispositivo móvil

Actualmente usamos celulares inteligentes y tabletas en la vida cotidiana. Los usamos para conectarnos, hacer compras, trabajar, hacer transacciones bancarias, seguir nuestra condición física y realizar cientos de tareas en cualquier momento, y desde cualquiera lugar.

¿Qué puede suceder si mi dispositivo móvil es atacado, se pierde o me lo roban?

- Puede ser utilizado por ciberdelincuentes para robarle su dinero o identidad. Para lograrlo, utilizan la información guardada en su dispositivo, incluso las cuentas de medios sociales y correo electrónico.

- Puede que pierda datos irremplazables como fotos, notas o mensajes (si no tiene copias de seguridad).
- Los ciberdelincuentes pueden usar su número de teléfono para estafar a otras personas.

¿Cómo protejo mi dispositivo móvil?

Seguridad del dispositivo:

- **Trabe** su dispositivo con una frase de contraseña, PIN o código. Use algo que sea difícil de adivinar: los ciberdelincuentes pueden deducir fácilmente su fecha de nacimiento y patrones de bloqueo. Use una frase de contraseña para seguridad óptima (vea la página 6). Piense también en usar reconocimiento facial o una huella digital para destrabar su dispositivo.
- **Asegúrese** de que su dispositivo tenga seleccionado el bloqueo automático después de un tiempo de inactividad corto.
- **No** cargue su dispositivo en una estación de cargado pública, y evite los cargadores de terceros.
- **Trate** a su teléfono igual que su billetera. Manténgalo seguro y consigo en todo momento.

Seguridad del software y aplicaciones

- **Use** la función de actualización automática de su dispositivo para instalar actualizaciones nuevas de aplicaciones y del sistema operativo tan pronto como estén disponibles.
- **Seleccione** la opción del dispositivo que requiere una frase de contraseña o contraseña antes de instalar aplicaciones. Los controles para padres también se pueden usar para este propósito.
- **Examine** los permisos de privacidad cuando instale nuevas aplicaciones en su dispositivo, especialmente las aplicaciones gratuitas. Instale solamente aplicaciones de vendedores de buena reputación.

Seguridad de los datos:

- **Active** las funciones de trabado y borrado remoto automático, si su dispositivo las tiene.
- **Asegúrese** de suprimir exhaustivamente los datos personales de su dispositivo antes de venderlo o deshacerse de él.

Seguridad de la conectividad:

- **Apague** Bluetooth y Wifi cuando no los esté usando.
- **Asegúrese** de que su dispositivo no se conecte automáticamente a nuevas redes de wifi.

Encontrará información más detallada sobre cómo proteger su celular bajo “Secure your mobile phone” en cyber.gov.au

Desarrolle su pensamiento ciberseguro

La ciberseguridad personal no se limita al cambio de selecciones; también incluye el cambio de su forma de pensar y de su conducta.

Cuidado con las ciberestafas

Se sabe que los ciberdelincuentes usan e-mail, mensajes, medios sociales o llamadas telefónicas para tratar de estafar a la población australiana. Estos delincuentes podrían fingir ser una persona u organización que usted cree que conoce, o que piensa que es de confianza.

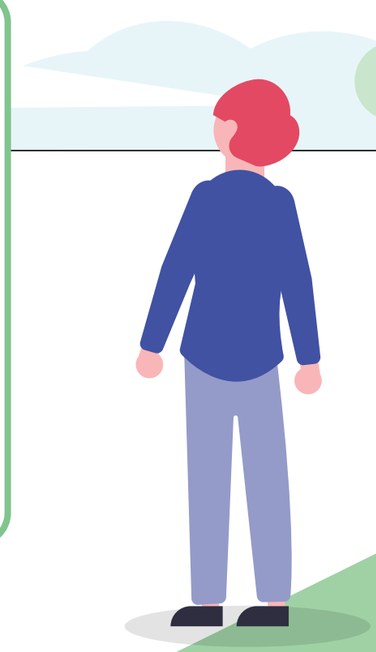
Sus mensajes y llamadas intentan engañarle para que haga ciertas cosas, por ejemplo:

- Revelar datos de cuentas de banco, contraseñas y números de tarjetas de crédito,
- Dar acceso remoto a su computadora,
- Abrir un archivo adjunto que podría contener malware,
- Enviar dinero o tarjetas de regalo.

¿Cómo puedo reconocer los mensajes de estafa?

Puede resultar difícil reconocer los mensajes de estafa. Los ciberdelincuentes suelen usar ciertos métodos para engañar. Sus mensajes pueden incluir los siguientes:

- **Autoridad:** ¿dice el mensaje que proviene de una fuente oficial, como su banco?
- **Urgencia:** ¿le dice que hay un problema, o que tiene un tiempo limitado para responder o pagar?
- **Emoción:** ¿despierta el mensaje en usted sensaciones de pánico, ilusión o curiosidad?
- **Escasez:** ¿le ofrece el mensaje algo que escasea, o le promete una buena oferta?
- **Actualidades:** ¿se refiere el mensaje a una noticia de actualidad o a un evento importante?



Aprenda a detectar mensajes fraudulentos o de phishing: visite “Learn the basics” en cyber.gov.au

¿Qué debería hacer si recibo un mensaje fraudulento?

Si recibe un mensaje o llamada telefónica fraudulentos, ignórelos, suprímalos o denúncielos a Scamwatch de ACCC en scamwatch.gov.au

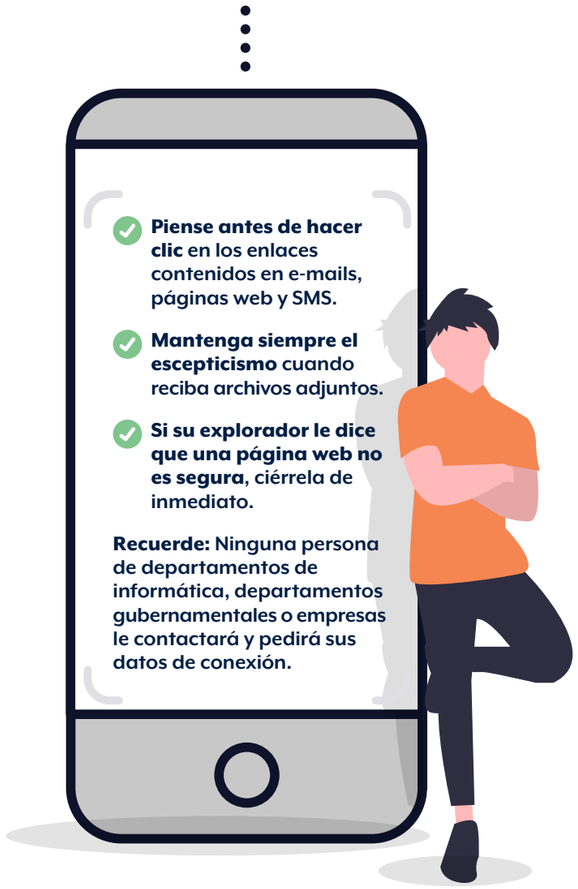
También puede llamar al número de ciberseguridad del ACSC al **1300 CYBER1** (1300 292 371) si le preocupa su ciberseguridad.

Si se ha involucrado con una estafa y piensa que esto es un riesgo para sus cuentas de banco y tarjetas de crédito o débito, póngase en contacto con su institución financiera inmediatamente. Es posible que ésta pueda cerrar su cuenta o detener una transacción.

¿Qué debo hacer si no estoy seguro/a si un mensaje es una estafa?

Si usted piensa que un mensaje o llamada podría ser realmente de una organización que le inspira confianza (como su banco) busque un método de contacto de confianza. Busque la página web oficial, llame al número de teléfono publicado o visite una tienda o sucursal. No use los enlaces o datos de contacto contenidos en el mensaje que recibió o que le dieron por teléfono, ya que podrían ser fraudulentos.

Sugerencia:
Piense antes de hacer clic.



- **Piense antes de hacer clic en los enlaces contenidos en e-mails, páginas web y SMS.**
- **Mantenga siempre el escepticismo cuando reciba archivos adjuntos.**
- **Si su explorador le dice que una página web no es segura, ciérrela de inmediato.**

Recuerde: Ninguna persona de departamentos de informática, departamentos gubernamentales o empresas le contactará y pedirá sus datos de conexión.

Si piensa que ha sido víctima de ciberdelincuencia, denúncielo por medio de ReportCyber del ACSC en cyber.gov.au/report o llame al número de ciberseguridad al 1300 CYBER1 (1300 292 371).

También puede mantenerse informado sobre los peligros más recientes: suscríbase al servicio gratuito de alertas del ACSC. Busque "Subscribe to the ACSC alert service" en cyber.gov.au
Le enviaremos una alerta cuando identifiquemos un nuevo peligro cibernético.

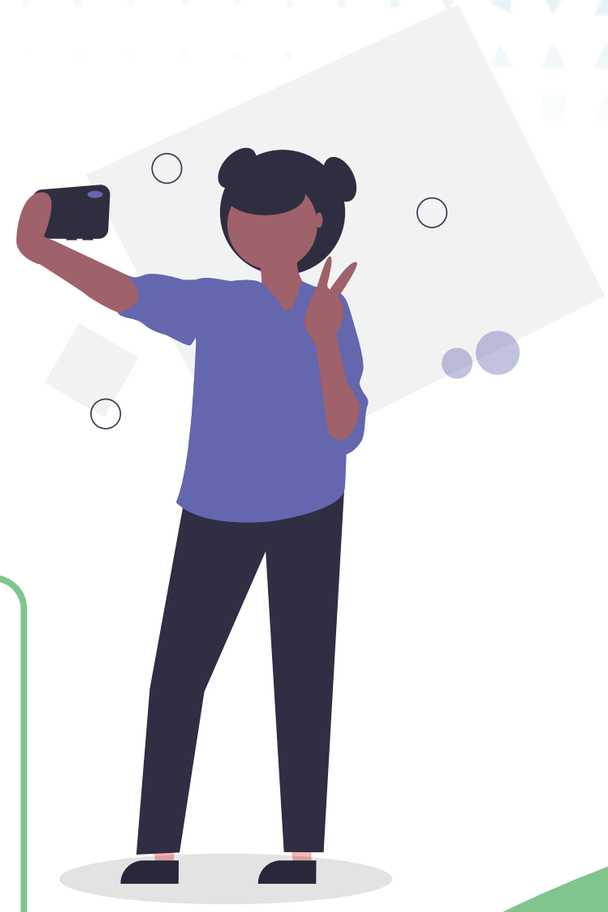
Deténgase y piense antes de compartir información en los medios sociales

Los ciberdelincuentes pueden usar la información que usted publique en su/s cuenta/s de medios sociales en sus estafas y ciberataques.

Recuerde que la información en internet es permanente y que nunca podrá suprimir completamente lo que haya publicado.

¿Cómo hago para detenerme y pensar antes de publicar?

- **Piense:** ¿Cómo podría un ciberdelincuente usar esta información para atacarme o atacar mis cuentas?
- **Piense:** ¿Me incomodaría mostrar esta información o imagen a una persona totalmente desconocida fuera de línea?



¿Qué información no debería compartir?

Evite compartir información (incluso fotos) en línea que los ciberdelincuentes puedan usar para identificarle, manipularle en una estafa o adivinar sus preguntas de recuperación de una cuenta. Esto puede incluir los siguientes:

- Lugar de nacimiento y fecha de nacimiento.
- Dirección y número de teléfono.
- Empleador e historial laboral.
- Dónde fue a la escuela.
- Cualquier otra información personal que se pueda utilizar para atacarle.

Lista de verificación resumida

¿Ha realizado todo lo que aparece en esta guía?

Use esta práctica lista de verificación para seguir su progreso:

- **He activado las actualizaciones automáticas en todos mis dispositivos:**
  - Computadoras (de escritorio y portátil).
  - Teléfono celular.
  - Tableta.
- **He activado la autenticación multifactorial en mis cuentas más importantes:**
  - Todas mis cuentas en línea de transacciones bancarias y financieras (p.ej. su banco, PayPal).
  - Todas mis cuentas de correo electrónico (p.ej. Gmail, Outlook, Hotmail, Yahoo!).
- **Hago copias de seguridad de mis dispositivos regularmente:**
  - Computadora (de escritorio y portátil).
  - Teléfono celular.
  - Tableta.
- **Uso frases de contraseña únicas y resistentes en mis cuentas más importantes que no están protegidas por MFA:**
  - Cuentas en línea de transacciones bancarias y financieras.
  - Cuentas de correo electrónico.
- **He protegido mis dispositivos móviles:**
  - Computadora portátil.
  - Teléfono celular.
  - Tableta.
- **Aplico procesos de pensamiento ciberseguros todos los días:**
  - Sé reconocer mensajes de estafa.
  - Sé qué hacer si recibo un mensaje de estafa.
  - Sé cómo comprobar si un mensaje es fraudulento (una estafa) si no estoy seguro/a.
  - Pienso antes de hacer clic en enlaces y archivos adjuntos.
  - Pienso antes de compartir material en los medios sociales.
- **Sé dónde obtener ayuda si soy víctima de ciberdelincuencia o de una estafa.**

Glosario

Acceso a distancia
Obtener acceso y control de dispositivos y redes fuera del sitio.

Aplicación
También conocida como aplicación de celular, aplicación define el software utilizado comúnmente en los teléfonos celulares inteligentes o tabletas.

Aplicación de autenticación
Una aplicación utilizada para confirmar la identidad de un usuario de computadora y darle acceso por medio de la autenticación multifactorial (MFA).

Archivo adjunto
Un archivo enviado con un mensaje de e-mail.

Ciberdelincuente
Todo individuo que piratea ilegalmente un sistema informático para causar daños o robar información.

Dispositivo
Un dispositivo de computación o comunicación. Por ejemplo, una computadora, computadora portátil, teléfono celular o tableta.

Fin de la asistencia
Fin de la asistencia se refiere a la situación en que una compañía cesa la asistencia para un producto o servicio. En general, esto sucede con productos de equipo y software cuando una compañía lanza una nueva versión y pone fin a la asistencia que ofrece para las versiones anteriores.

Malware
Software malicioso utilizado para conseguir acceso no autorizado y control de la computadora de un usuario, robar información y perturbar o desactivar redes.

Nube
Una red de servidores remotos que ofrece almacenamiento distribuido y poder de tratamiento de datos masivos.

Recuperación de cuenta
Un proceso que utiliza una serie de preguntas u otros métodos de verificación para recuperar o volver a tener acceso a una cuenta o para cambiar la frase de contraseña o contraseña de una cuenta.

Sistema operativo
Software instalado en el disco duro de la computadora que le permite a ésta comunicarse con sus programas y ejecutarlos. Ejemplos: Microsoft Windows, Apple macOS, iOS, Android.

Software
Conocidos comúnmente como programas, una colección de instrucciones que permiten al usuario interactuar con una computadora, su equipo o realizar tareas.

Testigo físico
Dispositivo físico que normalmente cabe en un llavero, que genera un código de seguridad utilizado para confirmar la identidad de un usuario de computadora que usa MFA.

Descargo de responsabilidad
El material en esta guía es de naturaleza general y no debe tomarse como asesoramiento jurídico o como ayuda para circunstancias determinadas o situaciones de emergencia. Para cualquier asunto importante, obtenga asesoramiento profesional independiente apropiado para su situación.

El Gobierno Federal no acepta responsabilidad alguna por daños, pérdidas o gastos que resulten de haber dependido de la información contenida en esta guía.

Obtenga más información o denuncie un incidente de ciberseguridad en:

cyber.gov.au | 1300 CYBER1 (1300 292 371)
Este número es para llamadas en Australia únicamente.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre