**Resumen de la presentación en línea**

Australian Government

Be Connected
Every Australian online.

# Manejar sus correos electrónicos de forma segura (Managing your emails safely)

Tener una dirección de correo electrónico es su puerta de entrada al mundo del Internet. Le permite mantenerse en contacto con familiares y amigos, y acceder a servicios como la banca y las compras en línea. Es importante que mantenga su cuenta de correo electrónico lo más segura posible, utilizando una frase de contraseña segura y autenticación multifactor.

## Formas de acceder al correo electrónico

Hay muchas formas de acceder a sus correos electrónicos. Puede hacerlo a través de:

### Una aplicación

- utilice la aplicación del proveedor de correo electrónico que puede descargar de App Store para dispositivos Apple, o de la Play Store para dispositivos Android
- vincule su cuenta de correo electrónico a:
  - la aplicación de correo preinstalada en su dispositivo inteligente
  - la aplicación Mail o Outlook de su computadora.

### Página web

- ingrese al sitio web de su proveedor de correo electrónico desde un navegador en su computadora o dispositivo inteligente.

## Proveedores de servicios de correo electrónico

Hay muchos proveedores de servicios de correo electrónico que ofrecen cuentas gratuitas y de pago, entre ellos:

- **Gmail** Google
- **Outlook** Microsoft
- **Yahoo Mail** Yahoo
- **iCloud** Apple
- **ProntonMail** Proton AG

Visite el sitio web de Be Connected para obtener guías paso a paso sobre cómo configurar y utilizar Gmail, Outlook y Yahoo.

**Sugerencia:** Puede que le interese crear una cuenta de correo electrónico sólo para sus operaciones bancarias o para realizar compras en línea, con el fin de gestionar mejor el correo basura.

# Manejo de su cuenta de correo electrónico

## Configurar carpetas y etiquetas

Crear carpetas en la bandeja de entrada es una buena forma de mantener su cuenta organizada y de localizar fácilmente los mensajes importantes cuando los necesite. Las carpetas a veces se denominan etiquetas, dependiendo del servicio de correo electrónico que utilice.

## Organizar y archivar sus correos electrónicos

Su servicio de correo electrónico dispone de controles prácticos que le ayudan a archivar los mensajes de distintas formas y a reducir al mínimo el spam y los correos basura. Cuando llega un nuevo correo electrónico y lo abre para leerlo, aparecen algunos controles en la parte superior de la pantalla. Puede hacer clic en estos controles para:

- **Borrar**: mover el mensaje a la papelera
- **Archivar**: mover el correo electrónico al archivo
- **Marcar como no leído**: hacer que el correo electrónico se marque como correo nuevo
- **Etiquetas/Carpeta**: etiquete el correo electrónico o póngalo en una carpeta.

## Manejo del correo basura

Su servicio de correo electrónico detecta y desvía automáticamente el correo electrónico no deseado conocido, pero aún así puede recibir algo de spam.

Si considera que un correo electrónico de su bandeja de entrada es basura o spam, puede:

- **Reportar spam**: reporte a su proveedor de correo electrónico que el mensaje es spam
- **Bloquear correos electrónicos**: deje de recibir correos electrónicos de ese remitente
- **Darse de baja**: dejar de recibir boletines o correos electrónicos de marketing a los que se haya suscrito.

Si cree que se ha dado de baja, pero sigue recibiendo spam, puede presentar una queja a la **Australian Communications and Media Authority (Autoridad Australiana de Comunicaciones y Medios de Comunicación)**.

> **Consejo:** Para evitar correos electrónicos no deseados, piénselo dos veces antes de facilitar sus datos para concursos. También reconsidere no dejar con marca las casillas que aparecen premarcadas para recibir correos de marketing cuando compre productos o servicios.

# Mantenga segura su cuenta de correo electrónico

## Frases de contraseña

Mantenga sus cuentas seguras con frases de contraseñas seguras. Las frases de contraseña son la versión más segura de las contraseñas y se componen de cuatro o más palabras aleatorias.

Intente pensar en una frase de contraseña diferente para cada una de sus cuentas y no recicle partes de ninguna antigua.

Cuando elija su frase de contraseña, esta debe tener las siguientes características:

- **Larga**: al menos 14 caracteres
- **Impredecible**: utilice cuatro o más palabras al azar con números, símbolos y letras mayúsculas y minúsculas
- **Única**: no reutilice sus frases de contraseña.

*Por ejemplo: Amarillo Asi Hey Planta > Amaril!*-ASiheyPl@nta!*

**Consejo:** Una aplicación de gestión de contraseñas también puede ayudarle a crear y almacenar contraseñas complejas que sean difíciles de adivinar o hackear. Puede encontrar información sobre **aplicaciones de manejo de contraseñas** y cómo configurarlas en el sitio web de Be Connected.

### Autenticación multifactor

Siempre es una buena idea activar la autenticación multifactor para sus cuentas. La autenticación multifactor (también conocida como autenticación de 2 pasos) añade una capa adicional de seguridad. Eso significa que, cuando inicia sesión en una cuenta con su contraseña, es posible que se le pida que complete un paso adicional para confirmar que se trate de usted, como introducir un código de un mensaje de texto o utilizar la identificación por reconocimiento facial.

### Utilice la seguridad de los dispositivos

Utilizar software de seguridad en su computadora es una de las formas más sencillas de proteger sus cuentas y dispositivos. Tener una buena seguridad para su computadora incluye la instalación de programas antiespía (anti-spyware), antivirus y cortafuegos (firewall) de confianza. También debe mantener actualizadas sus herramientas y aplicaciones de seguridad en línea activando las actualizaciones automáticas.

### Utilice una conexión segura

Cuando necesite acceder a sus cuentas, enviar información sensible o introducir contraseñas, conéctese a una conexión a Internet de confianza; por ejemplo, desde casa, en el trabajo o utilizando los datos de su celular si están disponibles. Las redes Wi-Fi públicas no son tan seguras como las de casa o el trabajo.

### Opciones de recuperación de cuenta

Asegúrese de establecer un número de teléfono de recuperación o una dirección de correo electrónico alternativa para todas sus cuentas de correo electrónico. Si pierde el acceso a su cuenta, o esta se ve amenazada, puede restablecer su contraseña utilizando su opción de recuperación.

## Correos electrónicos fraudulentos

Los correos electrónicos fraudulentos están diseñados para que parezcan de organizaciones legítimas que usted conoce. Pueden parecer reales, utilizando logotipos y una dirección de correo electrónico similar a la de la organización por la que se hacen pasar. Los correos electrónicos fraudulentos pueden parecer del banco, del proveedor de servicios de Internet, de un organismo público, de un vendedor o incluso de un estafador que se hace pasar por un amigo o un familiar. Al hacerse pasar por alguien de confianza, los estafadores utilizan la sensación de urgencia para engañarle y conseguir que pague dinero o facilite información personal, como contraseñas importantes o datos bancarios o de tarjetas de crédito.

Este tipo de estafas se denominan estafas de suplantación de identidad o correos electrónicos de phishing.

## Consejos para evitar correos electrónicos fraudulentos

- Esté atento/a a señales de que un correo electrónico es fraudulento. Los correos electrónicos fraudulentos pueden:
  - expresar una sensación de urgencia o utilizar tácticas intimidatorias, exigiendo un pago o pidiéndole que confirme datos personales;
  - utilizar saludos genéricos como “Estimado cliente”, “Estimado usuario” o no utilizar ningún saludo;
  - pedirle que haga clic en un enlace o que descargue un archivo, lo cual podría dirigirle a un sitio web falso o contener un virus o software malicioso.
- Compruebe siempre que la dirección de correo electrónico del remitente sea legítima y póngase en contacto directamente con la organización consultando su sitio web oficial y su número de teléfono.
- Nunca ingrese a sus cuentas en línea ni verifique datos a través de un enlace en un correo electrónico, ni haga clic en enlaces o abra archivos adjuntos en correos electrónicos de remitentes desconocidos o que sean sospechosos.
- Elimine los correos sospechosos o que puedan ser una estafa, utilice la opción “denunciar spam” para clasificarlo como correo no deseado.

**Consejo:** Si desconfía de un correo electrónico, hable con un amigo o familiar de confianza y póngase en contacto con la organización a través del número de teléfono que aparece en su sitio web.

Visite el sitio web Be Connected para consultar nuestra **guía gratuita sobre estafas de suplantación de identidad** elaborada con Scamwatch.

# Tómese su tiempo para explorar Be Connected

Be Connected es un sitio web integral con recursos gratuitos diseñados específicamente para ayudar a los australianos mayores a conectarse a Internet de forma segura y a navegar por el mundo digital con confianza. El sitio también es útil para familias y organizaciones comunitarias que quieran ayudar a miembros mayores de la comunidad a acceder a todas las ventajas de Internet.


## Visite beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Este programa ha sido desarrollado por el Comisionado de eSafety como parte de la iniciativa Be Connected.