



Información proporcionada por Instituto de Previsión Social

Campaña Más vale prevenir

Última actualización: 27 enero, 2026

Descripción

La campaña "**Más vale prevenir**" es una iniciativa impulsada por ChileAtiende y el Instituto de Previsión Social (IPS), con el objetivo de informarte sobre los fraudes del momento, especialmente a través de correos, mensajes de texto, SMS y llamadas telefónica.

Revisa las recomendaciones y consejos para evitar distintos tipos de fraude en el [sitio web del IPS](#).

Revisa los tipos de fraude

Si bien existen cientos de estafas, las más comunes son:

Pagos pendientes:

Llamado telefónico de un supuesto funcionario de gobierno, que indica que tienes pagos pendientes. Para el depósito, piden tu cuenta y clave del banco. Sin embargo, las instituciones del Estado, cuando hacen estos llamados, **no piden datos bancarios**, solamente informan.

Falso pago inmediato de un beneficio:

Es un llamado telefónico de un supuesto funcionario de ChileAtiende el cual te indica que para agilizar el retiro de un beneficio y su posterior depósito, debes entregar tus claves bancarias. **Esto es un fraude.**

Supuesto "pago rápido" con un clic:

Es un mensaje de texto al teléfono o un correo electrónico, que indica que debes hacer clic en un vínculo, donde te piden tu cuenta y clave del banco. No abras ni pinches el link o botón. Debes **borrar el mensaje de inmediato**, porque es una estafa.



- Informar a través de medios de prensa.
- Publicar recomendaciones de seguridad en el sitio web del IPS para el buen uso de tecnologías.
- Publicar mensajes en redes sociales del IPS y ChileAtiende aconsejando los tipos de fraudes.
- Reforzar los contenidos de apoyo para los canales de atención IPS y ChileAtiende para la entrega de recomendaciones.
- Coordinación con organismos como el Servicio Nacional del Adulto Mayor (SENAMA) para tomar acciones conjuntas y dar recomendaciones a los adultos mayores.



- Para consultar o solicitar beneficios, accede solo a sitios web institucionales conocidos y de confianza. Siempre ingresa escribiendo la dirección o URL completa en la barra del navegador, fijándote que aparezca.
- Los trámites digitales del IPS, por ejemplo, se realizan siempre por los sitios oficiales y, en algunos casos, por vía remota con adecuados procedimientos de identificación de las funcionarias y funcionarios.

Correos electrónicos o SMS al celular:

- No abras vínculos que lleguen dentro del mensaje, ni hagas clic en botones asociados a mensajes de este tipo que soliciten datos bancarios, en relación con beneficios del Estado. En estos casos, es mejor borrar el mensaje.
- Los trámites para solicitar beneficios del Estado se hacen a través de sitios web oficiales o con adecuados mecanismos de autenticación.

Llamadas telefónicas:

- Cuando digan que llaman de una institución pública, no entregue datos como: número de serie de tu [cédula de identidad](#) o claves del banco.
- Desconfía cuando te pidan datos de autenticación, aunque la voz se escuche amigable. Cuelga y no tengas miedo a ser descortés.
- Las llamadas de servicios públicos no están orientadas a pedir datos bancarios, sino que a fines informativos.

Redes sociales:

- No dejes tus perfiles abiertos cuando terminas de ocupar algún dispositivo. Cambia tus claves de forma permanente.
- No entregues tus datos personales a través de mensajes públicos. Utiliza mensajes privados o DM.
- Ubica y sigue las cuentas oficiales del IPS o instituciones bancarias que paguen tus beneficios o pensión.

Cajeros automáticos:

- No insertes tu tarjeta cuando sospeches de personas desconocidas o si ves objetos extraños en el teclado, la ranura o el lector de la tarjeta.
- Protege tu contraseña con la mano y no aceptes indicaciones de uso del cajero por parte de desconocidos.

Locales de pagos y sucursales:

- Solo consulta al personal autorizado con sus respectivas credenciales.
- No cuentes tu dinero fuera del local.
- No recibas alimentos ni bebidas de extraños fuera de una sucursal.
- No transites por lugares solitarios o poco frecuentes.

Importante: si te ocurre algo similar a lo indicado y tienes dudas, verifica siempre en los canales oficiales de las instituciones relacionadas. En el caso de ChileAtiende, pregunta directamente en nuestras redes sociales o en el call center **101** o al **+56 4 4236 20 00** (si estás en el extranjero). Revisa el [horario de atención](#).



de Carabineros o al 134 de la Policía de Investigaciones (PDI).

Si prefieres, ingresa una denuncia a través de cualquier unidad policial o del Ministerio Público.

Entérate sobre los términos digitales

- **Barra del navegador:** es el lugar donde se digitan o escriben las direcciones o URL de los sitios web.
- **Cuentas verificadas:** es una insignia de cuenta verificada (ticket azul), que indica que las cuentas de redes sociales son oficiales y que representan a organismos estatales, entidades privadas y personajes públicos, entre otros.
- **DM:** significa “mensaje directo” y es privado en las redes sociales.
- **Datos personales:** información que puede ser usada para identificar de forma directa o indirecta a una persona, como su nombre, fotografía, número de teléfono, dirección particular y RUN, entre otros.
- **Phishing:** práctica utilizada por cibercriminales (hackers) para la captación de datos personales a través de Internet. De ese modo, pueden suplantar la identidad de las personas para acceder a sus cuentas bancarias o usar sus identidades para cometer ilícitos.
- **Remitente:** es quien envía un correo electrónico, pudiendo ser una persona, una entidad pública o un organismo privado, entre otros.
- **Tarjetas de coordenadas:** tarjeta entregada por el banco, que sirve para realizar operaciones que impliquen movimiento de fondos (dinero) o contratación de productos y servicios a distancia.

Obtén más información u orientación

Si tienes dudas:

- Solicita una [videoatención en ChileAtiende](#).
- Llama a al call center ChileAtiende **101** o al **+56 44 236 20 00** (si estás en el extranjero). Revisa el [horario de atención](#).
- Dirígete a una [sucursal ChileAtiende](#) con tu [cédula de identidad](#).