



**Evita estafas al usar tus
dispositivos móviles**

**Empoderamiento
digital**

Con el apoyo de



Los dispositivos móviles son herramientas tecnológicas que puedes llevar contigo y usar en distintos lugares. Funcionan con batería recargable y conexión a internet. Algunos ejemplos son teléfonos inteligentes, tabletas, computadoras portátiles y relojes inteligentes.

Usarlos puede ayudarte a comunicarte, consultar información, hacer pagos o realizar trámites. Para aprovecharlos con tranquilidad, conviene que conozcas medidas sencillas para prevenir estafas y ciberataques.

1

¿Cómo operan los estafadores y ciberdelincuentes?



Quienes cometen fraudes usan distintas técnicas para obtener información personal, contraseñas, dinero o acceso a cuentas.

1

Investigan a sus víctimas antes de atacar. Analizan redes sociales, datos públicos, contactos, actividades, gustos, etc.

2

Provocan miedo, urgencia o confusión para que la persona actúe rápido, sin revisar con calma. Por ejemplo: "¡Urgente! Se bloqueará tu cuenta".

3

Envían correos, mensajes de texto o códigos QR con enlaces o archivos maliciosos para robar información o cuentas de WhatsApp o redes sociales.

4

Suplantando la identidad de instituciones públicas, financieras, aseguradoras, aerolíneas, compañías de internet o telefonía, celebridades y familiares (incluso recrean la voz con inteligencia artificial)

5

Con el pretexto de dar apoyo técnico, piden compartir pantalla o instalar programas de acceso remoto. Así pueden ver información privada o controlar el equipo a distancia.

¿Qué medidas podrías implementar para prevenir estafas y ataques cibernéticos?

Para utilizar de manera segura tus dispositivos móviles, te recomendamos hacer lo siguiente:

1. Usa contraseñas fuertes (password)



- a) **Protege** tus dispositivos con contraseñas.
- b) **Evita usar la misma contraseña** para diferentes dispositivos o accesos.
- c) **No utilices datos personales** como ciudad o país de nacimiento, fechas importantes, nombres de mascotas o familiares, o números seguidos como 1, 2, 3, 4. Son fáciles de adivinar.
- d) Crea contraseñas con **frases largas**, fáciles de recordar y difíciles de adivinar. Por ejemplo: elbosquedeencinos. Son más seguras si:

- Combinan letras mayúsculas y minúsculas, por ejemplo:
ElBosqueDeEncinos.

- Usan combinaciones poco comunes o imaginativas, por ejemplo:
BosqueDeTrebolesGigantes.



Para recordarlas, puedes anotarlas en una libreta y **guardarla en un lugar seguro** al que solo tú tengas acceso, como un cajón con llave. Evita escribir junto a la contraseña el nombre exacto de la cuenta o aplicación.

También podrías considerar:



Tu código de activación es *****



Usar un gestor de contraseñas, herramienta que ayuda a guardarlas y completarlas de forma segura. Un ejemplo es **Google Password Manager**.

Usar códigos de un solo uso enviados por mensaje, cuando la cuenta lo permita.

Usar opciones de seguridad como el reconocimiento de voz o facial, si tu dispositivo las tiene disponibles.

2. Fortalece la seguridad de tus dispositivos



- a) **Actualiza** con frecuencia el sistema operativo y las aplicaciones para evitar fallas de seguridad.
- b) En tu computadora portátil y tabletas, instala un **antivirus** y mantenlo actualizado.

También puedes activar la **verificación** en dos pasos: dos formas de confirmar tu identidad, por ejemplo, una contraseña y un código enviado a tu teléfono.

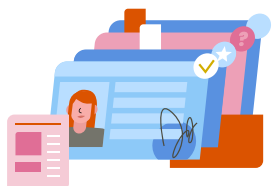
Si lo necesitas, pide a una persona de confianza que te apoye con las configuraciones de seguridad de tus dispositivos móviles.



3. Cuida tu información confidencial y sensible



- a) **No compartas información personal** en llamadas, mensajes, perfiles, estados o historias de WhatsApp o redes sociales, como:



Nombre y apellidos, fecha y lugar de nacimiento, correo electrónico, domicilio personal o de trabajo, número de teléfono, identificaciones oficiales o información de familiares.



Datos de tarjetas, códigos de seguridad, claves de acceso, contraseñas o códigos de verificación.

- b) Configura la **privacidad** de tus publicaciones en redes sociales o WhatsApp y evita compartirlas con el público en general.
- c) En redes sociales no aceptes solicitudes de amistad de **personas desconocidas**.
- d) Si usas un dispositivo compartido, como una computadora familiar o del trabajo, **cierra tus sesiones** de correo, redes sociales, portales o aplicaciones financieras al terminar.



4. Mantente alerta



- a) **Activa notificaciones** de transacciones en tus cuentas financieras y tarjetas para identificar operaciones que no realizaste.
- b) **Recibir** una transferencia de dinero es **automático**: no requiere que aceptes o autorices la operación.

5. Desconfía y analiza



- a) Para comprar en línea o usar portales y aplicaciones financieras, utiliza **redes privadas** o los **datos** de tu teléfono.
- b) No contestes llamadas ni abras mensajes de números desconocidos.
- c) **Revisa los destinatarios de los correos**. Las entidades oficiales, como instituciones financieras, no usan dominios de Gmail o Outlook.
- d) **No sigas enlaces sospechosos**. Para entrar a un sitio oficial, escribe tú mismo la dirección en el navegador. Verifica que comience con https y muestre una señal de sitio seguro, como un candado.
- e) **Evita abrir fotos o descargar archivos adjuntos** que vengan de personas o direcciones **sospechosas**.
- f) **No permitas que otras personas vinculen sus dispositivos** a tu cuenta de WhatsApp.
- g) **Desconfía de premios, ofertas o inversiones** demasiado buenas para ser verdad. Por ejemplo: premios que piden pagar primero un impuesto, cancelación inmediata de deudas, renovaciones del hogar gratuitas, inversiones con rendimientos milagrosos o trabajos para ganar mucho dinero fácilmente.



Estas recomendaciones son un punto de partida. Dependiendo de cada situación, pueden implementarse muchas otras medidas de prevención.



3 ¿Qué hacer ante una posible estafa o un ciberataque?

Si sospechas de una estafa o ciberataque, detente, conserva la calma y haz lo siguiente:

- a) Si recibes una **llamada sospechosa** de un supuesto familiar, **cuelga**. Luego llama directamente a esa persona o a alguien de confianza que confirme la situación.
- b) Si recibes una llamada sospechosa de una institución, **no compartas datos**. Busca sus números oficiales y llama directamente para verificar.
- c) Si el **ataque** está relacionado con un producto o servicio de una institución financiera, por ejemplo, compras en línea que no realizaste:

Revisa si el cargo fue aplicado por tu institución financiera.

Bloquea la tarjeta desde la aplicación de la institución financiera o marca al número que viene en la tarjeta o en el sitio web oficial.

Reporta con tu institución financiera la operación que no reconoces.

Cambia tus contraseñas.

- d) Si tu institución financiera no da seguimiento oportuno, **contacta a la entidad responsable** de proteger a las personas usuarias de servicios financieros en tu país.
- e) **Denuncia** ante la policía nacional o la fiscalía de tu localidad. Si fue un ciberataque, acude a la unidad especializada en delitos informáticos o ciberdelincuencia, si existe en tu país.
- f) **No calles** por pena o miedo. Al denunciar, ayudas a que otras personas también estén protegidas.
- g) **Habla sobre lo que te pasó** con familiares o amigos de confianza.



Recuerda: usar tus dispositivos móviles con seguridad te permite seguir conectado, informado y aprovechar sus beneficios. Para cuidarte:



1. Protege tus accesos y dispositivos.

2. Cuida tu información personal y confidencial.

3. Desconfía de mensajes, llamadas y solicitudes sospechosas.

Con el apoyo de

