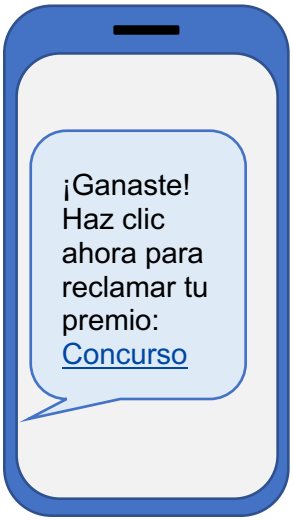
Grassroots Digital Hub

Consejos de seguridad para el teléfono



Tenga cuidado con…

- Llamadas y mensajes SMS/texto de números que no conoce.
- Mensajes que lo hagan sentir muy feliz o asustado.
- Una llamada o mensaje que lo presione para actuar rápidamente.
- Un SMS/texto que le indique hacer clic en un enlace.
- Si hay demora antes de que el llamante comience a hablar.
- Si un llamante es abusivo o amenazante.
- Cualquier solicitud de dinero o información personal/confidencial.

No lo haga!

- No proporcione información confidencial, como su Número de Seguro Social (SIN – Social Insurance Number), información bancaria o nombre de usuario y contraseña.
- No envíe dinero.
- No haga clic en los enlaces que le envíen.
- No responda al SMS/texto.
- No llame al número que le dan ni use la función de devolución de llamada de su teléfono.

Qué hacer

- Está bien colgar o dejar que un llamante desconocido vaya al buzón de voz.
- Bloquee el número.
- Si le preocupa un ser querido, busque su número y llámelo directamente.

Recuerde

- Los estafadores pueden ser muy astutos y harán todo lo posible para manipularlo, incluso hacerse pasar por seres queridos.
- Una empresa que lo presiona no merece su negocio.

- El gobierno y los bancos no solicitan información personal por teléfono si lo llaman. Si usted los llama, pueden pedirle esta información para verificar su identidad.

Lo que podría ver o escuchar

- **Una súplica de ayuda:** Parece que es alguien que conoce y que realmente necesita su ayuda, usualmente dinero. Le dicen que si no ayuda, algo malo les ocurrirá.
    - El llamante o SMS/texto gana su confianza mediante:
        - Compartir información personal sobre usted y su familia (que encontraron en redes sociales)
        - Sonar exactamente como alguien que usted conoce (esto podría ser IA – Inteligencia Artificial)
- **La amenaza:** El llamante o SMS/texto es agresivo y exigente. Podrían decirle:
    - Que es el gobierno o un servicio legal contactándolo
    - Que algo muy malo pasará si no actúa de inmediato
    - Que debe visitar un sitio web o compartir información confidencial, como su SIN o información bancaria
- **Buenas noticias!** El llamante o SMS/texto puede decir que tiene una gran oferta solo para usted, que ganó un concurso o que recibirá dinero. Pueden volverse agresivos o abusivos si hace preguntas o se demora. Podrían decirle que debe:
    - Actuar rápido
    - Hacer clic en un enlace o proporcionar información personal
- **Una oferta de ayuda:** El llamante o SMS/texto puede decir que es su banco o servicio de informática. Podrían decirle que:
    - Su dispositivo o cuenta ha sido hackeado (“comprometido”)
    - Para recibir ayuda, debe hacer clic en un enlace o proporcionar información confidencial
    - Si se demora, perderá sus fondos o servicios

Si te ocurre a ti

- Si compartiste tu nombre de usuario y contraseña, intenta cambiarlos de inmediato.
- Si compartiste información bancaria o de tarjeta de crédito, llama a tu banco de inmediato.
- Haz un informe a la policía y al Canadian Anti-Fraud Centre’s online reporting system (Centro Canadiense Antifraude sistema de denuncia en línea) o por teléfono al 1-888-495-8501.
- Informa a tus amigos y familiares lo que te ocurrió para que sea menos probable que les pase a ellos.

SSHRC CRSH
Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
NSERC CRSNG
We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council.