



CIBERCONSEJOS ADULTOS MAYORES



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática



Adultos mayores seguros en línea

¡En internet, siempre debemos estar alertas para evitar engaños! Por eso, le llamamos a seguir estos consejos:

- Compre sólo en sitios oficiales. Cuidado con vendedores en lugares como Instagram o Facebook. Si decide comprar ahí, exija medios de pago formales y busque si existen reclamos contra ellos en línea antes de comprar.
- No entregue información personal, financiera o claves, tampoco códigos recibidos por WhatsApp o mensaje de texto, por mucho que alguien asegure ser de su banco o alguna institución similar de confianza. Podría ser una estafa.

Adultos mayores seguros en línea

- Use contraseñas diferentes para cada cuenta, que sean fáciles de recordar, pero difíciles de adivinar. Por ejemplo, usando tres palabras no relacionadas como clave.
- Tenga cuidado con la información que compartes en internet, podría ser usada por delincuentes. Evite publicar o entregar a otros datos personales como la dirección, el RUT y la fecha de nacimiento.
- Proteja el acceso a su celular con una medida de bloqueo como un PIN o, idealmente, la huella digital o el reconocimiento facial, para dificultar que terceros accedan a su información personal.

Adultos mayores seguros en línea

- Evite las redes wifi abiertas (como las de cafés o negocios) al hacer compras o transacciones financieras. Haga estas transacciones con su internet de la casa o celular.
- No transfiera dinero a personas que lo soliciten de manera urgente, asegurando ser familiares, policías o miembros de alguna institución. Existen fraudes en los que se asegura tener contenido privado de la víctima con tal de extorsionarla: es mentira.
- Desconfíe de audios o videos que invitan a invertir dinero. Suelen ser fraudes que suplantán la imagen de personalidades famosas para convencer de invertir en estafas.

Adultos mayores seguros en línea

- No haga clic en enlaces ni descargue archivos sin estar seguro de que proceden de una fuente confiable, podría tratarse de un phishing.

¿Qué es un phishing?

Son mensajes que envían delincuentes haciéndose pasar por personas u organismos de confianza. Llaman a hacer clic en un enlace o descargar un archivo, muchas veces con mensajes urgentes, como citaciones pendientes o situaciones bancarias irregulares.

¡No lo haga! Contacte directamente a la institución si cree que el mensaje pueda ser real.