

¡Siga estos consejos principales para mantenerse seguro en línea!

UTILICE CONTRASEÑAS SEGURAS...

Sus contraseñas deben ser:

Largas: 16 caracteres como mínimo

Complejas: utilice letras mayúsculas y minúsculas, números y símbolos

Únicas: utilice una contraseña diferente para cada cuenta



... Y UN ADMINISTRADOR DE CONTRASEÑAS

Los administradores de contraseñas pueden:

- Guardar todas sus contraseñas
- Avisarle cuando sus contraseñas sean débiles o si las ha reutilizado
- Generar contraseñas seguras para usted
- Rellenar automáticamente la información de acceso a sitios y aplicaciones

ACTIVE LA AUTENTICACIÓN MULTIFACTOR



Proporciona **una capa de seguridad adicional** al confirmar su identidad cuando accede a cuentas, por ejemplo, ingresando un código enviado por mensaje de texto a un teléfono o generado por una aplicación de autenticación.

RECONOZCA Y DENUNCIE LA SUPLANTACIÓN DE IDENTIDAD

Las señales más comunes de un mensaje de suplantación de identidad incluyen:

- Lenguaje urgente/alarmante
- Solicitudes de información personal o financiera
- Mala redacción o faltas de ortografía
- Direcciones de correo electrónico o enlaces incorrectos



¿Identificó un mensaje de suplantación de identidad?

Denúncielo y luego elimínelo



ACTUALICE SU SOFTWARE

Las actualizaciones de software garantizan que sus dispositivos estén protegidos frente a las amenazas más recientes. ¡Active las **actualizaciones automáticas** en la configuración de seguridad de su dispositivo o aplicación!