CIBERSEGURIDAD
Universidad Nacional del Comahue

Recomendaciones de Seguridad para el Uso de Redes Sociales

Aplicando estas prácticas, puedes proteger tu seguridad y privacidad al usar redes sociales, reduciendo riesgos como el robo de identidad, el acoso o las estafas en línea.

- Evita contactarte con desconocidos: No aceptes solicitudes de amistad ni interactúes con perfiles que no puedas verificar como legítimos.
- Verifica cualquier información recibida: Antes de compartir o reaccionar a una publicación, asegúrate de que la información provenga de una fuente confiable.
- Revisa la configuración de privacidad: Asegúrate de que solo tus amigos o contactos seleccionados puedan ver tu información personal, publicaciones y fotos.
- Configura la autenticación en dos pasos (2FA): Habilita el doble factor de autenticación para proteger tu cuenta contra accesos no autorizados.
- Mantén actualizada la información de recuperación de cuentas: Verifica que el correo alternativo y el número de teléfono de recuperación estén actualizados y sean accesibles solo por ti.
- Limita la información personal expuesta: Evita incluir datos sensibles en tu perfil, como dirección, número de teléfono o fecha completa de nacimiento. Revisa regularmente quién puede ver esta información.
- Ten cuidado con la publicación de fotos: Revisa que las fotos no contengan información sensible (e.g., documentos, ubicación geolocalizada). Piensa en el contexto antes de publicar.
- Limita los permisos otorgados a aplicaciones de terceros: Al vincular aplicaciones a tus redes sociales, revisa qué datos están solicitando y elimina permisos innecesarios.
- No hagas clic en enlaces sospechosos: Evita enlaces acortados o poco claros, incluso si provienen de contactos. Los perfiles de amigos también pueden ser hackeados.
- Evita responder mensajes sospechosos o cadenas: Las cadenas de mensajes suelen ser tácticas para propagar desinformación o malware.
- Desconfía de premios o sorteos demasiado buenos para ser verdad:
- Muchas estafas se hacen pasar por concursos legítimos en redes sociales para obtener tus datos personales.

- Revisa el historial de inicios de sesión: La mayoría de las plataformas permiten verificar dispositivos conectados. Cierra las sesiones desconocidas.
- No publiques información en tiempo real sobre tu ubicación: Compartir que estás de viaje o en eventos puede exponer tu ausencia y ser aprovechado por personas malintencionadas.
- Sé crítico con los desafíos o retos virales: Algunos de estos retos buscan acceder a tus datos personales o manipularte para realizar acciones perjudiciales.
- Cambia tus contraseñas regularmente: Utiliza contraseñas únicas y complejas para tus cuentas de redes sociales, preferiblemente gestionadas con un administrador de contraseñas.
- Monitorea los datos compartidos por tus contactos: Si alguien etiqueta o menciona información personal tuya, revisa las publicaciones para proteger tu privacidad.