

# PRECAUCIONES EN LAS REDES SOCIALES

En las redes sociales generalmente se incluyen datos sensibles o personales que dan a conocer los gustos, costumbres, lugares que se frecuentan, fotografías y amigos, por lo que se deben tomar en cuenta precauciones de lo que se comparte, debido a que podrían producir casos de **violación a la privacidad, usurpación de perfil, robo de identidad, acoso, extorsión y mucho más.**

Se recomienda configurar las opciones apropiadas de seguridad y tomar todas las precauciones necesarias para evitar la vulnerabilidad y amenazas expuestas en Internet.

Al formar parte de una red social se recomienda tener las siguientes precauciones:

- Conozca bien las condiciones y términos de uso de la red social en la que desea tener un perfil o cuenta.
- Sea cuidadoso con la información personal que comparte, ya que puede ser pública.
- Sea discreto publicando la menor cantidad de información personal.
- Seleccione bien los "amigos" que se admiten y los que se siguen.
- Realice una minuciosa configuración de las opciones de privacidad de manera precisa para configurar su cuenta.
- Proteja los álbumes de fotos y videos para tener un mayor control de quién puede ver el contenido.
- Evite compartir contenidos de terceros si no está seguro de la veracidad de la información.
- Tenga cuidado con lo que escribe. Evite bromas o comentarios inadecuados que puedan traer consecuencias a nivel personal y profesional. Haga un uso responsable de las redes.
- Esté atento ante comportamientos extraños.
- Evite utilizar computadoras o redes inalámbricas públicas para ingresar a redes sociales.
- Siempre cierre las sesiones en cada red social o correo electrónico.
- Cuidado con el GPS y la localización, ya que podría adjuntar información de ubicación a cualquier contenido multimedia que envíe o reciba. Twitter, Facebook e Instagram usan esta característica extensivamente para ayudar a los usuarios a indicar la ubicación donde se hizo una foto.
- Proteja lo mejor posible la información de contacto para evitar robo de información que pueda ser usada en su contra. Los métodos más utilizados son a través de la Ingeniería Social (donde los delincuentes buscan extraer información a través del vínculo, la "amistad" o cualquier comunicación que permita la red social).
- Otra forma de robo de información es por medio de la Información Pública (la cual se basa en una mala configuración de las redes sociales y que permite que la información de índole personal esté accesible aún sin estar entre los amigos o escogidos como "seguidores". Los cibercriminales buscan este tipo de descuidos para apropiarse de dicha información).

Las redes sociales tienen sus beneficios y sus riesgos, por lo que se deben utilizar de forma cuidadosa y responsable. Para más información, ver panfleto Seguridad en redes sociales, <https://ci.ucr.ac.cr/ciberseguridad>

