

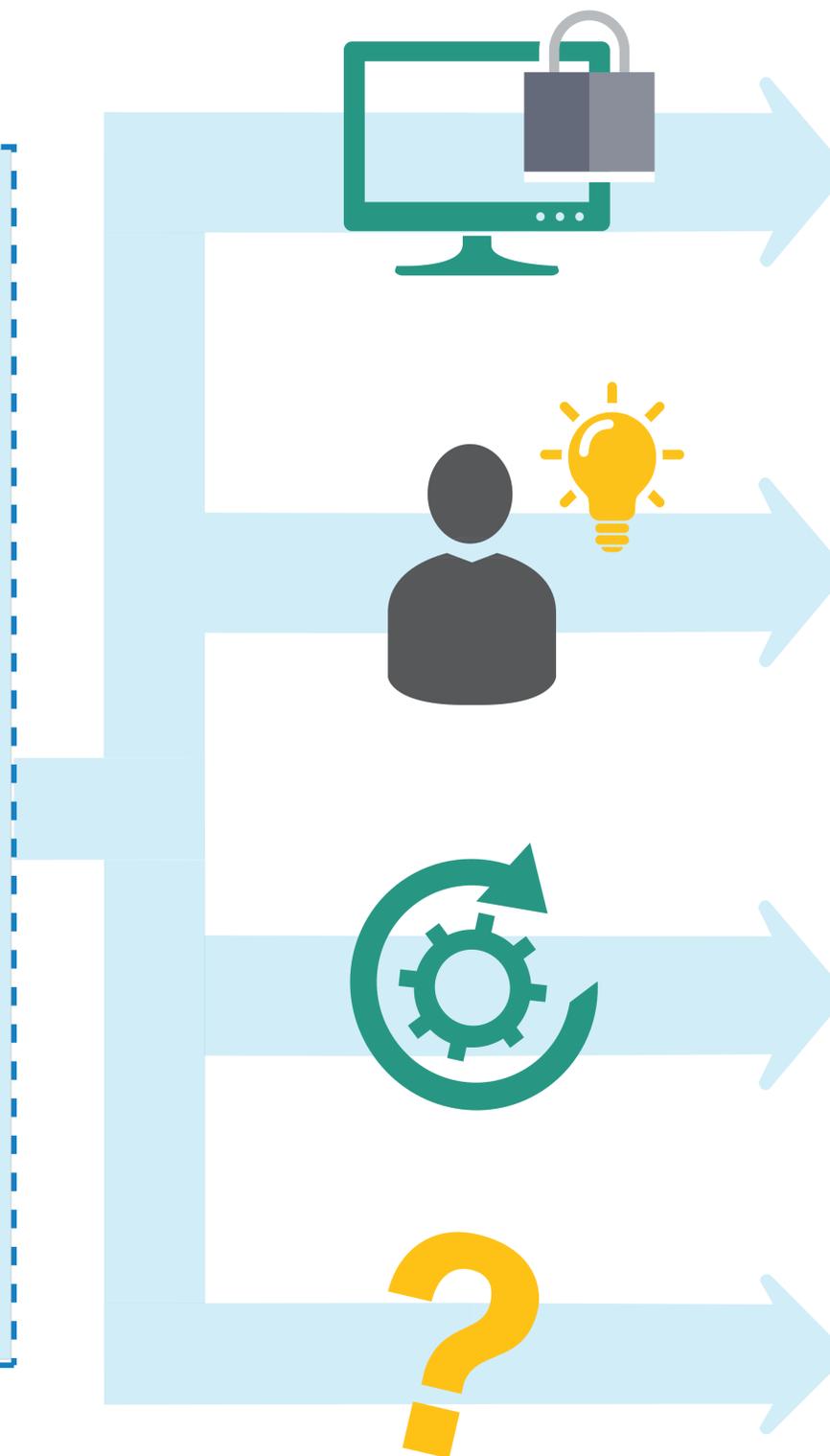
In the last couple of years we've all become increasingly reliant on Internet technology that uses our physical location to, for example, find directions, search for restaurants, shops and attractions in a particular place and even to collect points, rewards and money saving discounts.

Services that combine social networking with your physical location ('geosocial networking') have become very popular because they help users connect with friends, family and other contacts in their local area.

There's nothing wrong with using these services, as long as you know what's happening with your data, and what disclosing your physical location could mean for your personal security.

Some services have built-in privacy features which enable you to share your location only with friends, family, or professional contacts – essentially only those within your social circle – and you can choose who sees this information.

However, some services make your data available to third party app developers, meaning that people who don't know you could see your profile information, photos and even your physical location. This could put the safety of some people at risk, particularly children.



What you can do to protect yourself

TAKE CONTROL. Check the privacy settings of your social media profiles to make sure that you are only sharing updates, photos and other data with people that you want to.

BE AWARE. If you're using a geosocial app on your smartphone or tablet, make sure you know whether you can switch your location on or off. If you don't want your location revealed, switch it off! Many services also include the ability to opt out of being included in people's public listings at particular locations or in friends' updates. If you don't want this information made public, you can opt out by changing your account settings.

KEEP UP TO DATE. With new apps constantly being released, it can be difficult to know which ones have access to information on your location. Review your account settings on a regular basis, and remove any third party applications you no longer use.

ASK QUESTIONS. If you're a parent of a child with a mobile device, make sure they understand the risks of sharing their physical location, and that they know how to control how much of their information people see online.