Data Protection 101

10 tips to keep in mind

1 Review privacy settings on social media accounts

Make sure whatever you post is visible only to friends, since anything that is public can be used to infer a lot about your private life. Be careful about whom you accept as a friend.

2 Don't be overconfident about your privacy settings

Privacy settings are not foolproof. One known bug allows some Instagram photos shared to Twitter from a private account to be viewed by anyone, including non-followers who click on the Twitter link.

3 Respect your friends' privacy

Photos that include other people affect their privacy as well as your own. While a group selfie at work might be acceptable, a photo from a late-night party might be less appropriate. It is good practice to check with your friends before posting such photos.

4 Children have privacy rights too

Uploading photos of children is a controversial issue, since by definition, children cannot give consent, and thus each image technically breaches their privacy. As a rule of thumb, avoid sharing images that show children who are not your own. And public images, taken in a restaurant, for instance, are preferable over private settings.

5 Protect your kids' data

Posting pictures of kids on their birthdays reveals information that could lead to leakage in later years. Also, a commonly used "secret" for bank or credit card accounts is the mother's maiden name, information that can be deduced from a parent's social media posts.

6 Always remember your audience

With hundreds or sometimes thousands of friends or followers, it is easy to forget who can see your posts, especially if you share content with "friends of friends" or the public. Before posting anything, ask yourself whether you would mind if your spouse, relatives or boss could read that text or see that image.

7 The Internet never forgets

Always assume that anything you have posted or uploaded to the Internet is available for years to come. Most companies merely hide content rather than deleting it, and content can quickly and easily be copied or downloaded before it disappears. Maintaining one's privacy is difficult, but getting it back is almost impossible.

8 Don't give out personal info in exchange for freebies

A free gift or service might entice you to share your data, but doing so can lead to unwanted emails, text messages or sales calls. Worse, with enough data, someone can impersonate you online and buy things in your name, or commit a crime and frame you for it.

9 Be careful about scanning payment QR codes

Scammers have started using fake QR codes to steal data and money from users, sticking their own code over a merchant's original one. Scanning a fake QR code could lead to your information being leaked.

10 Be careful about downloading apps to your mobile phone

Many apps require a lot of intrusive control or access to your data. If an app is asking for more information than it should need to do its job, give it a miss.

Source: NUS Centre for Research in Privacy Technologies