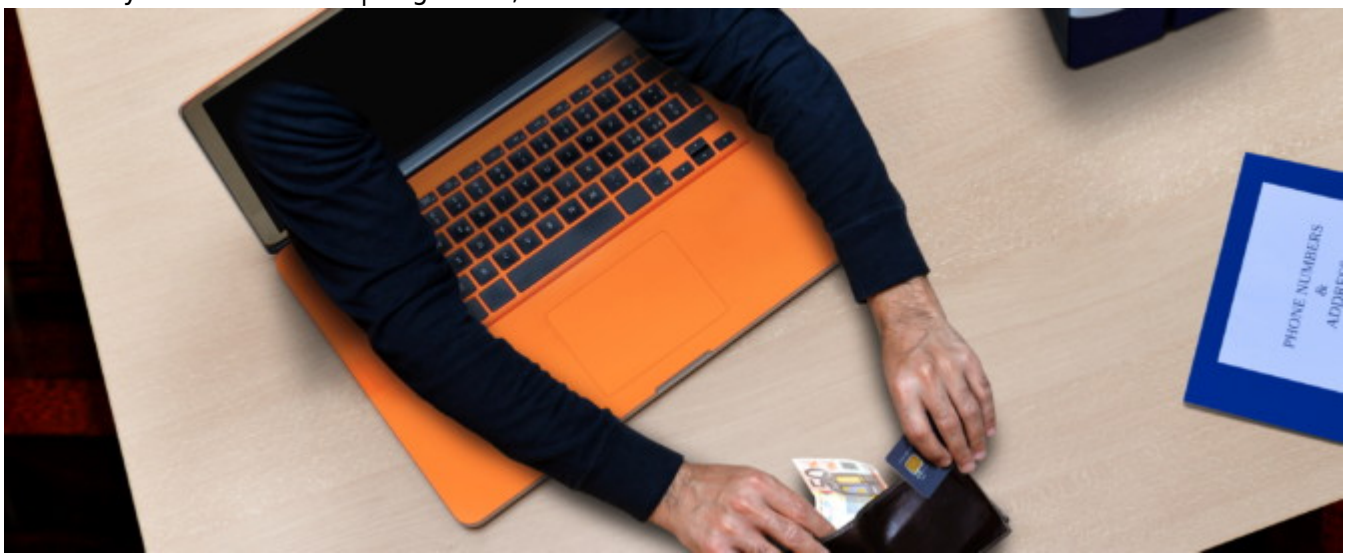
5 WAYS TO PROTECT PERSONAL INFORMATION WHILE USING CLOUD SOFTWARE

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Sasha Beharilal | August 16, 2017



Cloud technology has significantly changed the way we transfer and store information. By allowing us to store our files in a space with no physical boundaries, cloud technology allows us to have access to any file at any time and from anywhere. The only downside is the additional privacy risks involved with using a cloud system. In terms of the Protection of Personal Information Act (POPIA), a cloud provider will be considered an operator (a company that processes information on behalf of other companies) because it owns the infrastructure on which personal information is gathered, processed or stored. This means that the cloud provider has a responsibility to keep your information safe, but you should also take the necessary steps to avoid being hacked.

From a business perspective, protecting your client's personal information is imperative as there are legal consequences if you fail to do so. For individuals, protecting your personal information is just as important and could save you from embarrassment of having your sensitive photos and documents leaked.

Here are 5 effective ways you can make your cloud computing more secure whether you are in a business that processes other peoples' personal information or if you are an individual who stores personal information on the cloud.

1. **Be smart about your password**

Use a unique password for your cloud account that is comprised of lower and upper case letters, numbers, and symbols.

2. **Opt out of automatic backups**

Automatic data back-ups may be useful, but they could also be risky in terms of privacy. If your device is set to automatically backup each time you plug in your phone and connect to WiFi, it is uploading all of your images, videos, and other files that could contain content you would rather not put out there.

3. **Apply two-factor authentication**

By applying the two factor authentication to your cloud account, you protect your information from others by requiring both your password and a unique pin sent to your phone or email address when logging from a new device. The security precaution combines something only you should know (your password) with something only you should have (your phone).

4. **Remove credentials from old devices**

One critically important step to cloud security that many individuals neglect is to ensure that your cloud account is fully disabled from your device before your give it away or sell it.

5. **Avoid unreliable WiFi networks**

Free wifi is great, but connecting to public WiFi accounts can increase the likelihood of your accounts getting hacked.

If possible, try to avoid open WiFi networks and stick to those that are encrypted. When you're using an open network, be sure to use a VPN (virtual private network) to protect your browsing activity and only visit secure sites (marked with https).

Cloud computing has a multitude of benefits, such as cost savings, accessibility and disaster recovery, however, remember that there are risks involved and it is therefore it is important to use cloud storage securely.

For more good, clear, precise advice, contact us.