DATA PRIVACY NEW YEAR'S RESOLUTIONS

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucinda Botes | February 8, 2019



As we celebrate the beginning of the digital decade, most of us usually take time to clean out our homes and get organised. A space in our lives that is usually missed and not thought of, is the digital space that we occupy.

This guide is to help you to get your Data Privacy in order and organised for the year ahead.

A massive collection of email addresses was leaked online last January. The data breach known as Collection#1 exposed about 772,904,991 unique email addresses and more than 21 million unique passwords.

The breach shows just how vulnerable we are online. To check whether your credentials have been exposed in the Collection#1 breach, visit the site "Have I Been Pwned". It allows you to type in your email address and check whether your data was affected in the Collection#1 data breach.

If you have been "pwned" the best solution is to change your password. When generating a password, you may want to consider using a password manager like 1Password, or LastPass. Password managers are useful tools that make it easy to generate secure unique passwords. It also allows you to store difficult passwords that you have generated so that you can access them whenever you want to log onto a site.

You may want to consider enabling two factor authentication ("2FA") on all your accounts including social media, banking and email accounts to add an extra layer of security.

The next step is to go through your app permissions and unclick all the permissions that you are uncomfortable with. For example, unclick the "track my location" options from Facebook or weather apps. Another good one would be to turn on the "do not track" option on Google Chrome.

Take the time to see what kind of information your accounts have on you. Facebook and WhatsApp now allow users to download their data history. This will show you how invasive certain apps are and may prompt you to delete them. If not, it is good to take stock of all your information that is out there.

Now that you've taken the time to get your digital house in order remember the following tips;

- Use secure passwords
- Enable two factor authentication
- Avoid using public Wi-Fi or use a VPN
- Turn off track location options in apps if possible.
- Be informed of the data that is kept on you.

If you or your organisation has experienced a data breach, we are able to advise on the legal and regulatory implications it may have. Contact us for more good, clear, precise advice.