Publication: Sowetan (JobMarket)
Publication Date: 09 Feb 2021
Page: 13

AVE: 260267.70
Circulation: 71797
Part: 1 of 1

Pay serious attention to what apps are asking you to do

Be careful of sharing personal and sensitive data over the net. /SUPPLIED

Be vigilant against solicitation for personal data

By **Londiwe Dlomo**

WhatsApp recently updated its privacy policy informing users that it will now be sharing information with parent company Facebook. WhatsApp has assured consumers that it is not reading your messages, it's just been noting your habits and engagements and is now going to share that information with Facebook.

This of course has caused anxiety among users but WhatsApp is not the only app that does this.

Google also notes your habits and countless other sites capture, store and analyse data. Most of the companies do this to secure their existing data, to improve customer experience and to make money.

So the only way to truly protect yourself is to go completely off the grid. But for those of us who need to stay online, here are some things you should be aware of;

"Firstly you should download your apps from a reputable place such as Google Play store. Then you should pay attention to the permissions that an app is asking you to grant it.

"If you're downloading a photo editing app it should not ask you for permission to your microphone etc," says Ilonka Badenhorst, managing director at mobile application service regulator Waspa.

Waspa – Wireless Application Service Providers' Association – is a "self-regulatory body with a mandate to represent and regulate its voluntary members, which provide mobile-based value added services [VAS]".

Waspa has a code of conduct for its volunteer members to adhere to, you as a consumer can contact it if you are subjected to unsolicited, unwanted marketing by one of its members.

It also has a Don't Call registry where you as a consumer can put your number free of charge so that you are not contacted by any of its members unless you specifically state otherwise.

Badenhorst says it is important to read what it is you're agreeing to when downloading apps or signing up on certain websites. She further advises that an individual should use incognito mode and regularly clear their web search and cookie history.

There are many companies that make a lot of money from selling consumer data. Most of this data is collected for consumer analysis but there is also a real danger of crime in the mining of your data.

People are often subjected to unsolicited marketing; others are exposed to phishing which is when you are sent an e-mail where the sender is trying to get sensitive personal data, often financial data, from the recipient. The SMS version of this is called smishing.

These types of crimes need the consumer to be extra vigilant and should you think that something is fishy, call your bank to confirm with them before doing anything the text is asking you to do.

"Oftentimes the username and passwords that consumers use to log into public WiFi are often the same logins they use everywhere else. And they think it's safe to do so but could be exposing themselves to criminals who then access those logins and use them to gain entry to their other accounts. It is advisable to use unique once-off logins when accessing things such as public WiFi," Badenhorst says.

Consumers should also boost their knowledge on what protections they have against their data being used inappropriately. In this country we have the Information Regulator among other bodies that monitors and enforces compliance by public and private bodies to act within the provisions of the Protection of Personal Information Act.

The PPI Act "aims to promote the protection of personal information processed by public and private bodies by, among others, introducing certain conditions for the lawful processing of personal information so as to establish minimum requirements for the processing of such information."