

Privacy and security tips for using health apps



Research before installing it

- Read independent reviews of the app and check the developers website to see if they are credible. If in doubt don't download the app.



Read the privacy policy and terms of use

- Who your data is shared with should be made clear in the policy. Also, a privacy policy doesn't mean your data will be private.



Avoid signing up with your Google or Facebook account

- Your information could be shared through these parties.



Be aware of permissions

- Be suspicious if an app asks for data not related to its main use, or asks for permission to access functions that seem unrelated.



Take care when sharing information

- Don't share your real name or any other personal information unless you're using a secure system.



Lock your phone

- Use a PIN or password to lock your phone – it's one of the best ways to protect your data. Set your phone to automatically lock when you're not using it.



Don't click on strange links

- Don't click on suspicious or unknown links or attachments.



Delete apps you're not using

- If you stop using an app, delete it. If the app allows, delete your account and other data.



Give feedback

- If you have been pestered by third parties or advertisers, send feedback to the developers and app stores.

For more information, scan the QR code or visit www.healthify.nz/apps/s/security-and-privacy-of-health-apps

