Waspa's Tips For Protecting Mobile Device Integrity

Online security is very topical with much advice dispensed regarding when not to click on fraudulent links, and how to identify imposter websites, for example. However, what of actual mobile device security?

In line with its consumer protection mandate, the Wireless Application Service Providers' Association of SA (WASPA) provides the following hints and tips for protecting the integrity of your mobile device:

- Don't give your mobile device an obvious identifying name. In the same way a hijacker might trawl the suburbs for certain vehicle brands, a device thief sitting innocuously at a restaurant table might very well be on the lookout for information visible via Bluetooth such as "Bob's_iPadAir2". It's risky to let the world know you're Bob and you have a R10 000 device on you.

- A lost or stolen mobile device without a password enabled is an invitation for trouble. It may be less hassle on a daily basis not to have to enter a four-digit password every time you wish to activate your mobile device but the risks if your device leaves your person are extreme. For example, some financial institutions still email bank statements to clients that simply require a click on a PDF attachment to open. Now imagine your bank statements culled from your on-device email account, coupled with a municipal invoice in your name, and that copy of your ID that many of us save on our devices. The result could be multiple store accounts opened in your name, and that would be the least of your identity theft problems.

- Some manufacturers allow the downloading of apps that enable you to locate a lost or stolen device. The 'Find My iPhone / iPad' app is an obvious example. However, have you ever tried to access this app remotely from another device - using another Operating System - when you really have lost your iPhone or iPad? WASPA's advice is to practice - before you've lost your phone, tablet or laptop.

- There really is 'an app for that' nowadays. Every commercial organisation wants you to download their app but it might be sensible mobile security advice not to download your bank's app, for example, and have it prominently displayed on your device. Some apps allow users to enter a watered-down version of their usual passcodes and, again, that's risky. There's also the fact that potential fraudsters can identify all the firms you do business with in one

glance. Rather consider accessing sensitive sites via your device's web browser. And enable Private Browsing so fraudsters don't have a virtual blueprint of your daily online life.

- Finally, turning off cookies and autofill will mean your mobile device will not automatically enter passwords and login information into websites you visit frequently, but this will also mean less of a privacy threat should your device quite literally fall into the wrong hands.