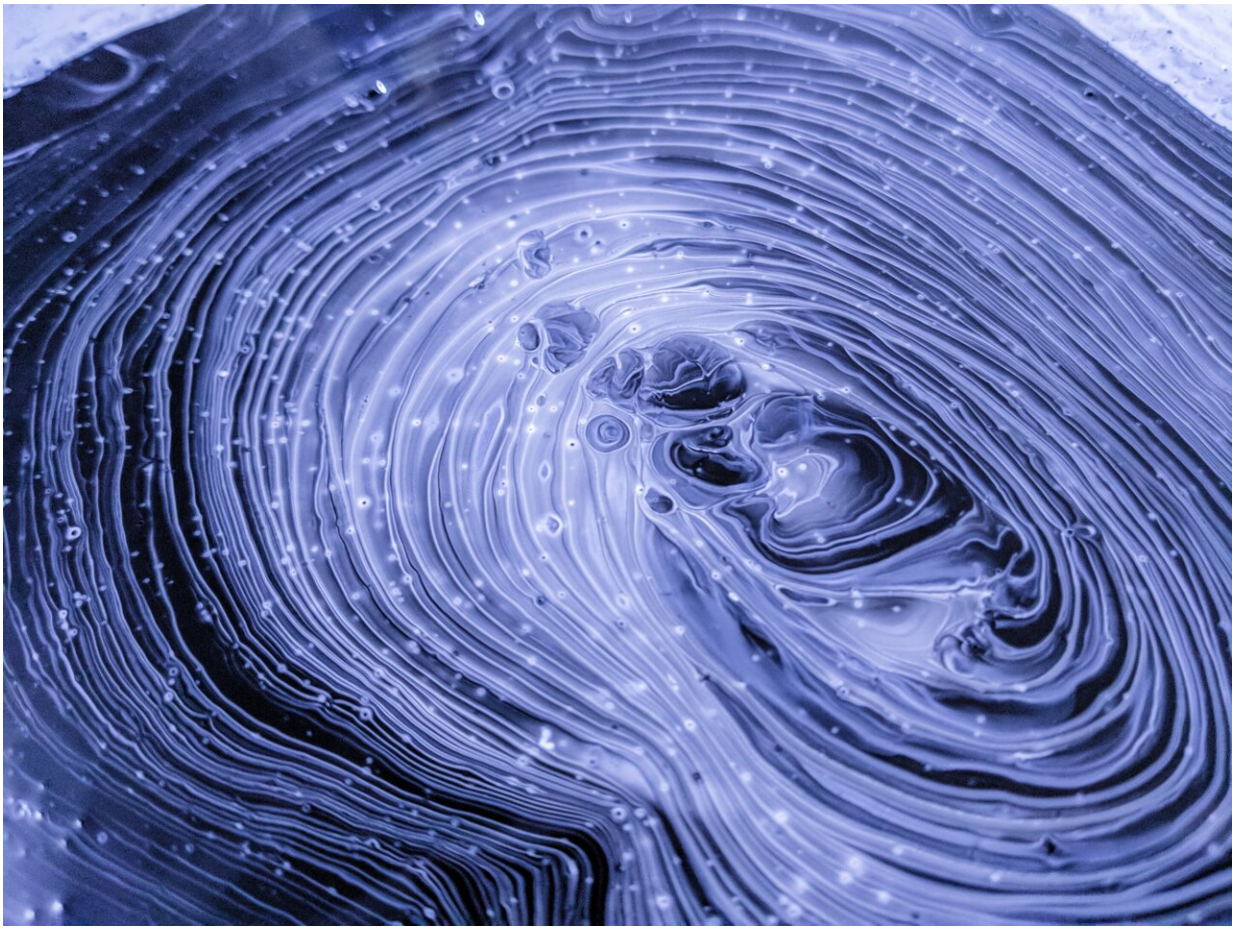
Some cybersecurity apps could be worse for privacy than nothing at all

October 22 2018, by Suranga Seneviratne



Credit: CC0 Public Domain

It's been a busy few weeks for cybersecurity researchers and reporters.

There was the Facebook hack, the Google plus data breach, and allegations that the Chinese government implanted spying chips in hardware components.

In the midst of all this, some other important news was overlooked. In early September, Apple removed several Trend Micro anti-malware tools from the Mac app store after they were found to be collecting unnecessary personal information from users, such as browser history. Trend Micro has now removed this function from the apps.

It's a good reminder that not all security apps will make your online movements more secure – and, in some cases, they could be worse than doing nothing at all. It's wise to do your due diligence before you download that ad-blocker or VPN – read on for some tips.

Security apps

There are range of tools people use to protect themselves from cyber threats:

- Virtual private networks (VPNs) allow you to establish a secure connection with a remote server and route all your traffic through it so it can't be tracked by your internet service provider. VPNs are commonly used to access geo-blocked content, and for additional privacy.
- Ad-blockers prevent advertisements from appearing on the websites you visit.
- App-lockers allow you to set passwords for individual apps. For example, if somebody borrowed your phone to make a call, and then tried to access your Facebook app.
- Tor hides your identity while you browse the internet, by encrypting and moving your traffic across multiple Tor nodes.

Know the risks

There are multiple dangers in using these kinds of security software, especially without the proper background knowledge. The risks include:

Accessing unnecessary data

Many security tools request access to your personal information. In many cases, they need to do this to protect your device. For example, antivirus software requires information such as browser history, personal files, and unique identifiers to function. But in some cases, tools request more access than they need for functionality. This was the case with the Trend Micro apps.

Creating a false sense of security

It makes sense that if you download a security app, you believe your online data is more secure. But sometimes mobile security tools don't provide security at the expected levels, or don't provide the claimed services at all. If you think you can install a state-of-the-art mobile malware detection tool and then take risks online, you are mistaken.

For example, a 2017 study showed it was not hard to create malware that can bypass 95% of commercial Android antivirus tools. Another study showed that 18% of mobile VPN apps did not encrypt user traffic at all. And if you are using Tor, there are many mistakes you can make that will compromise your anonymity and privacy – especially if you are not familiar with the Tor setup and try to modify its configurations.

Lately, there have been reports of fake antivirus software, which open backdoors for spyware, ransomware and adware, occupying the top spots on the app charts. Earlier this year it was reported that 20 million Google

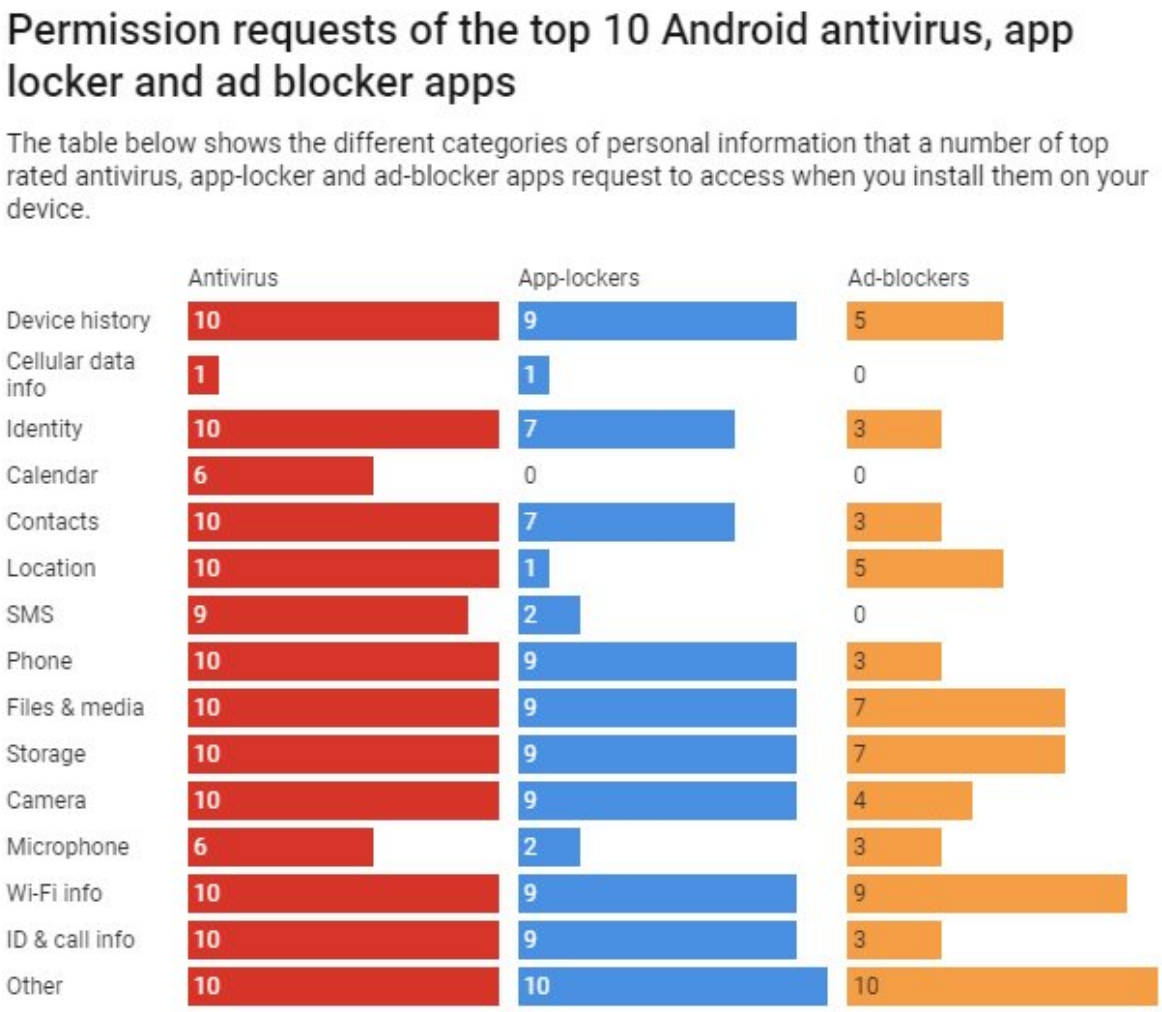
Chrome users had downloaded fake ad-blocker extensions.

Software going rogue

Numerous free – or paid – security software is available in app stores created by enthusiastic individual developers or small companies. While this software can provide handy features, they can be poorly maintained. More importantly, they can be hijacked or bought by attackers, and then used to harvest personal information or propagate malware. This mainly happens in the case of browser extensions.

Know what you're giving away

The table below shows what sort of personal data are being requested by the top-10 antivirus, app-locker and ad-blocking apps in the Android app store. As you can see, antivirus tools have access to almost all the data stored in the mobile phone.



Credit: Chart: Shelley Hepworth. Source: Google Play

That doesn't necessarily mean any of these apps are doing anything bad, but it's worth noting just how much personal information we are entrusting to these apps without knowing much about them.

How to be safer

Follow these pointers to do a better job of keeping your smart devices secure:

Consider whether you need a security app

If you stick to the official apps stores, install few apps, and browse only a routine set of websites, you probably don't need extra security software . Instead, simply stick to the security guidelines provided by the manufacturer, be diligent about updating your operating system, and don't click links from untrusted sources.

If you do, use antivirus software

But before you select one, read product descriptions and online reviews. Stick to solutions from well-known vendors. Find out what it does, and most importantly what it doesn't do. Then read the permissions it requests and see whether they make sense. Once installed, update the software as required.

Be careful with other security tools

Only install other security tools, such as ad-blockers, app-lockers and VPN clients, if it is absolutely necessary and you trust the developer. The returns from such software can be minimal when compared with the associated risks.

Provided by The Conversation