

NEVER install these on your phone

a little CRC

We have visits at the CRC every week from people who are worried their phone has been hacked. Almost all of them have some things in common: They have installed (often without intending to) one of the following apps:

PDF readers, QR code readers, Phone 'cleaners', and 'virus checkers' (or some other 'security' software)...

PDF readers

A PDF reader is almost certainly built into your phone already. Please don't take a chance by installing an unknown PDF reader from the app store.

To read a PDF on a Samsung phone you can use the built in OneDrive or Google PDF viewer, or 'Samsung Notes'. iPhones have their own built in PDF viewers and almost all Android phones do too.

If all else fails, install 'Adobe Acrobat Reader' using the Play Store or the App Store. It has adverts but is known to be legitimate and will allow you to fill in and sign digital forms. It will nag you to sign in or pay money. Just look for the 'X' to close and ignore these requests.

QR code readers

Almost all smartphones can read QR codes without you installing a new app. It's just a matter of finding where that existing capability is hiding.

On an iPhone or Samsung phone, just use the camera app. As you hover the camera over the QR code a link should appear on your screen which you can click on.

You can also read a QR code using Google Lens. Many phones have Google Lens installed on the phone home screen. It is the right hand icon here



The first time you use it you will need to give it permission to use your camera and access your photos.

Phone 'cleaners' and Virus Checkers

Phone 'cleaners' and 'virus checkers' are often installed as a result of fake popups aka Scareware scams.

A modern Android phone or an iPhone does not need a virus checker or cleaner. The number one reason for these apps to exist is to install malware and scam you.

There are a few legitimate phone security apps but you do not need them! Our experience is that even legitimate security apps inadvertently set people up to fall for scams. This advice applies to phones and computers.

None of us are invulnerable to security issues, no matter how much we know, no matter what security apps we use, and no matter how much we're prepared to pay to stay safe. We all need to learn good security instincts and practices. That's easier said than done so come into the CRC and get some coaching.

Good security practices relate to: passwords, backups of data/ photos/ etc, when to trust SMSs and emails, when NOT to click links, where to install software from, how to research if an app is trustworthy, and more. Help is often free and always cheap.

The Scareware Scam...



Scareware is an app or a web page which causes alarming warnings about fake threats, often disguised to look like a legitimate part of your operating system or anti-virus software. These warnings may pop-up over the top of everything and be hard to dismiss.

When you click a link or button, even a link like the 'I don't want to be safe' one above, you will be prompted to install useless or fake software including 'cleaner' and 'anti-virus' apps. It's all a scam and installing this software will compromise your security.

If your device appears to be locked on one of these messages, come and see us at the CRC. Often a small change to your notification settings fixes everything. We will also check your list of installed software to see if anything recently installed looks suspicious.