SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

App Security

Most people now use apps in some way. Whether you have a smartphone, laptop or even a smart TV, we can download third party apps which provide us with extra functionality. With apps being so popular and easily available, criminals will naturally look to exploit them, so it's important to take some simple steps to protect yourself.

Only download official apps

Whatever device you're using, you should only download apps from the official store.

These stores vet apps when they're submitted, and only allow them on once they've been checked for malicious code, and that they meet certain terms and conditions.

However, you should still be cautious when downloading apps from official stores - make sure it is the genuine app you're looking for and do your research before downloading anything.

Avoid downloading any apps from websites, as these haven't been checked and could contain malicious software. For example, there have recently been reports of fake symptom tracker apps, which are actually designed to steal information once installed.

Settings and permissions

Once you've downloaded an app, you'll need to review the settings and permissions.

When you first start an app it will usually ask for certain permissions such as access to the camera, contacts or photos, depending on what the app needs.

Rather than simply allowing access by default, take a minute to consider each option. Think about whether that app would need a certain permission (e.g. a photo app would probably need access to your camera), then decide whether you will allow permission or not.

Once you've set up the app, go into the settings and see what security and privacy settings you have available. You'll want to ensure that where possible, activity is either private, or only shown to those who you want to see it (for example, the friends mode on some social media).

You want to avoid having any activity as 'public' unless necessary.

Updates

Updates provide security patches against known weaknesses.

You should install software updates as soon as reasonably possible. Phones and tablets can often be set to update overnight when you're not using them.

Once an app has been updated, check the security settings for any new options, and in case any settings have reverted to the default options.

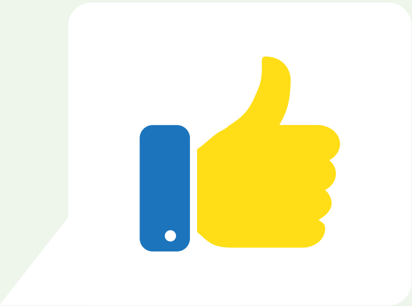
Review your apps

Every once in a while, look through your apps to see if you still use or need any you've previously downloaded.

As a general security rule, the more stuff you have on a device, the more vulnerabilities you introduce.

It's worth bearing this in mind for all of your devices.

Apps on work devices



You should only install approved apps on work devices. These apps will have been vetted and approved by your IT teams.

If you require an app which has not been approved, you should contact your IT team to discuss your requirements.

For more information on keeping your devices secure, see the National Cyber Security Centre (NCSC) web page at https://www.ncsc.gov.uk/guidance/securing-your-devices

swrocu.police.uk/cyber @swrccu SW Regional Cyber Crime Unit