Modified Apps – What are they and are they dangerous?

With the growing popularity of mobile applications, a new kind of app has emerged: Mod apps. Modded apps, Mod Apps, or Mod APKs are very popular in the Android world and are simply modified versions of the original mobile app. They are generally created in order to provide users with “better” features that are not available in a particular region or app already.

How safe are modified apps?

Modified apps are not developed by the original creator or the original app. They are often made by random individuals or groups of coders. For hackers and malicious attackers, this is a prime option to steal data from someone’s mobile device. The hacker can create a replica of a very popular application and make the features available to people who can’t afford to pay for the premium application for example, or who want additional features are not available in the original app.

Modified apps are mostly available from sources outside Android’s official app store (ie. Google Play Store). Therefore it is always advisable not to install any app on your mobile device that is downloaded from outside the Google Play Store. Often your mobile device will warn you when you go ahead with the process of installing an app from an untrusted source, and that is because of the security issues these apps present.

Not only can these modified apps be malicious in nature – infecting the device with a virus or stealing your personal data, but they can also aggressively push out advertisements with inappropriate content or redirect users to phishing sites.

WhatsApp Blue is an example of a modified app that we know pupils have become aware of. It promises additional “themes” if users are bored of the traditional WhatsApp green, the ability to send almost any form multimedia and promises additional privacy options and the option to send a message to an unsaved number for example.

How do we combat modified apps?

Modified app developers go to great lengths to make the app look as genuine as possible. So the following mitigations would be best practice:

- Only download and install apps from the Google Play Store
- Do check the developer’s background information (even if in the official app store)
- Check reviews from other users (although these too can be “faked”