NEBRC
NORTH EAST BUSINESS RESILIENCE CENTRE
CRIME PREVENTION IN A DIGITAL ERA

DOWNLOADING APPS

As there are various mobile device manufacturers and each device often has its own operating system, app stores vary depending on the device. This means that the way in which apps are downloaded and the permissions are subject to change.

✔ **Apps will ask for permissions to access different areas of your device.**

✘ **If you are unhappy with any app, remember you can always uninstall it!**

Android

Android is an open-source operating system owned by Google which uses the Play Store to download apps. Android is the only operating system of the top three which runs on many manufacturers' devices (Samsung, Sony, HTC etc.).

After downloading an app from the Play Store, it will ask for various permissions on your device. These permissions allow the application - from that request until permissions are later changed - to access different areas of the device. The Play Store, although governed by Google, is not as secure as it seems.

iOS

iOS is a closed source operating system owned by Apple which makes use of the AppStore to distribute applications. The AppStore has stricter policies regarding what applications can be added to it; although the fact that the security is greater does not make it perfect. This must be kept in mind when apps are being installed.

If an app requests more permissions than are granted by default, a pop-up screen will appear. From there you can choose which permission(s) you want to enable or disable.

Windows

On a Windows mobile, apps are kept in a sandbox environment. This technique isolates apps and prevents them from interacting with one another unless you have given permission for them to do so. Apps are available to be downloaded from the Windows App Store.

App permissions

Application permissions that may be asked for include:

- Camera
- Microphone
- Contacts
- Location
- Send and/or receive SMS texts
  Reads and/or writes to Storage (This one is common, allowing applications to create log files)
- Full Network Access (Allowing for Internet access over Mobile data or Wi-Fi) Keeping the device active (Not allowing the device to sleep for extended periods of time when inactive could do damage to the battery.)
- Access to device accounts (This may mean that they can access data stored in that account which may not be something you want.)

Many of these permissions apply to both Android and iOS but less so to Windows devices. When keeping track of app permissions, it is important to be conscious of what the app is meant to do. It is good practice, when apps ask for permissions, that they inform you why they need said permissions. This should help with the decision on whether or not to accept them. It is also important to note that there are free and paid versions of apps available. Ads are common with free apps and are one of the main causes for malware to be downloaded onto the device.