University Technology Services
University of South Carolina

Android Malware Removal

When an Android mobile device becomes infected, the cleanup is not as bad as you might think.

Backup the Device

Without backing up the device, users will likely lose all of their data. This may include photos, settings, contacts, and more. This step provides them with the opportunity to preserve that information.

Do not back up any applications or application data. An application is likely causing the infection. While inconvenent, it is necessary to purge all that data from the Android system.

This backup can be either physical (using a USB connection to a PC), or cloud-based.

Several mobile security providers offer backup services **free of charge.** A couple of the options are:

Easy App Toolbox
(Dropbox, Box, Google Drive)
Super backup
(PC or gmail attachment)
TrustGo Android AV

Some Android carriers offer comparible survices that are built-in to the device.

Wipe the Device

During this stage, we want to take the Android back to the factory settings. It should behave like a brand new phone after completion and restart.

Restore the Data

With the phone returned to factory condition, you can now use the backup to restore the user's information. **Do not restore any applications or application data to the device.** By doing so, the risk of reinfection is raised.

These procedures will vary, depending on the backup method the user selected earlier.

Prevent Future Infections

An unprotected Android device is no different than an unprotected computer. It is important that the system regularly receive (and install) updates for the operating system and applications.

Users should also install an anti-virus application. Anti-virus services offer greater protection, make it easier to backup and restore, and are often **free of charge**. There are countless products on the market, a few options include:

AVAST! Free Mobile Security
AVG AntiVirus FREE
TrustGo AntiVirus & Mobile Security

In the future, users should make sure they only download applications from a trusted app store.

Disclaimer:

The University Information Security Office (UISO) makes every effort to vett the products and instructions we recommend. Many of us use the listed products on our mobile devices. This document does not represent an endorsement of these products and services by the University of South Carolina. Due to the varience in devices and carriers, it is not possible for us to warrant this information.

UNIVERSITY OF SOUTH CAROLINA

http://security.sc.edu

The University of South Carolina is an equal opportunity institution.