Copies of legitimate apps are infected with malicious code and placed in official app stores.

3rd-party Apps

Unofficial websites where users can freely download applications. They are a general threat since there is no control over what applications are made available.
INSTALL ONLY APPLICATIONS YOU NEED
With every application installed, you increase the potential for vulnerabilities on your smartphone.

DOWNLOAD APPLICATIONS FROM TRUSTWORTHY SOURCES
Make sure to check the feedback from other users before installing the program from an app store.
Don’t grant ‘Trusted App status’ blindly.

http://kb.mcgill.ca/it/protect-your-mobile
WiFi and Other Connections
Keep optional network connections (e.g. WiFi and Bluetooth) turned off except when you are using them. Don’t leave your “WiFi ad-hoc mode” on.

NO PUBLIC WiFi
Don’t access banking or shopping sites over a public WiFi connection. Use WiFi-protected access on McGill campus (wpa.mcgill.ca) and in residences (wpa.rez.mcgill.ca).

http://kb.mcgill.ca/it/protect-your-mobile
HOW THEY GET YOU

SPYWARE
Silently collects information from users and sends it to eavesdroppers.

EXPLOITING
Some malware will exploit mobile platform vulnerabilities to gain control of the device.

WORM
A program that replicates itself, spreading throughout a network.

TROJAN
A program (or app) that seems to be legitimate, but is really malicious.

www.bullguard.com
KEEP ALL SOFTWARE UPDATED

Make sure to update the operating system and applications regularly. Updating your device ensures that it is protected from known threats.

WATCH OUT FOR SUSPICIOUS EMAILS

Don’t respond. Don’t open attachments. Don’t click on any embedded links.

WEB BROWSING

Limit your web browsing to well-known and trusted sites. Use SSL encryption (https://) for browsing and webmail whenever possible.

http://kb.mcgill.ca/it/protect-your-mobile