How an Adversary can Use a Smartphone for Surveillance, Access your Private Data, or Track your Location

If someone manages to install malicious software on your smartphone, you must assume it is then being used as a sophisticated surveillance and tracking device to read every text/SMS message, phone call, email, data file, and to capture anything you say or type on the keyboard. Even a non-compromised smartphone can be used by the government and/or phone company to track your location and eavesdrop on your conversations.

Outlined below are the six major ways in which your smartphone can be compromised and then used as a surveillance device or to capture your personal information. If you are security conscious, you must follow the advice given the document, "Essential Security for your Smartphone" in order to minimize the chance of your smartphone being compromised. ("How to Combat" numbers below refer to this document.)

1) **Malicious or Vulnerable Apps**: (How to combat: #1, #2, #3, #4, #10, #11, #13)
   a) Purposely downloading what appears to be legitimate software, but actually has hidden malicious elements.
   b) Or, legitimate apps that are vulnerable to attack because they have unpatched security holes that can be exploited by criminals or adversaries.

2) **Compromised Websites**: Visiting a seemingly legitimate website that installs malicious software on your device (How to combat: #1, #2, #3, #11, #13)
   a) Can be a legitimate website that has been hijacked (booby-trapped) by sophisticated hackers.
   b) Or can be a website set up to specifically fool you into visiting it with the purpose of installing malicious software.

3) **Unsolicited Malicious Links or Documents**: Being fooled to click on a booby-trapped document or website link. Contains elements of social engineering to fool you into clicking. (How to combat: #1, #2, #3, #4, #9, #13) -- Most common methods of fooling you are:
   a) Phishing emails. These may include:
      i) Malicious attachments, that install malware on your device just by opening them, even if they appear legitimate and include useful information
      ii) A website link (URL) that takes you to a website that has been designed to install malicious software or steal your personal information.
      iii) A website link or a document that then asks you to enter your username and password to gain access; this steals your credentials and the attacker can then get into your accounts.
   b) Text/SMS messages that have links to malicious websites like outlined above.
   c) Pop-ups that appear on your device when in public locations or when visiting a website. These pop-ups may be generated by a malicious website, or by networking equipment that has been hijacked in order to distribute malware.
      i) Generally don't trust pop-ups that tell you to update your software or install "security software", especially if this happens when visiting a website. Just reboot!
      ii) Never update software or phone settings in a public location (public WiFi).

4) **Physical Access**: Someone gaining physical control of your device and installing software (if it is temporarily confiscated, lost, or stolen). Without a strong PIN/Password and encryption, your device can be hacked into. (How to combat: #1, #5, #6, #7, #8, #9, #13, #15, #20, #21)
   a) It only takes a minute for an attacker to install surveillance software on your smartphone, especially if it is unlocked.

b) A sophisticated attacker, such as a state actor, may be able to install tracking software on your device even if it is apparently still locked.

5) **Government Surveillance**: Even if your smartphone is turned "OFF", it can be used to track your location and may also be used as a microphone to listen to your conversations. (How to combat: #19, #22, #23)
   a) An otherwise completely secure smartphone (or any phone) can be tracked by the government in conjunction with a local telephone company. They can track your location and identify all other phones near you, thus making connections between you and others, as well as track everywhere you go.
   b) The "Off" mode in modern-day phones is only a software setting, meaning that it is not truly off unless the battery is removed. Even in this off mode, the government (in conjunction with the local phone company) can use your phone as a listening device to hear all phone conversations.
   c) Any plain text/SMS message can be read by the government working in conjunction with the telephone company. (How to combat: #19)

6) **Preinstalled Apps**: Malicious or insecure apps that are pre-installed when you purchase your device (How to combat: #1, #2, #13)
   a) Suspect any device that has been opened or repackaged; malicious apps may have been installed.
   b) Any used device may have malicious or tracking software installed.
   c) Some countries (such as Russia or China) are moving to a model where any device sold within the country must have government sponsored software pre-installed.
   d) For Androids, phone manufacturers install their own software on smartphones, which are not part of the core Android operating system. Much of this software is not built with security in mind; it may be tracking you or may include vulnerabilities that can be exploited. But they cannot be removed or updated. (How to combat: If you buy an Android, get a Google Pixel.)

Examples and Resources for Further Research:

1) Blog post on Social Engineering: www.computersecuritynw.com/blog-1
2) Malware Delivered Via Fake Browser Updates Are Back and are More Sophisticated Than Ever: blog.knowbe4.com/malware-delivered-via-fake-browser-updates-are-back-and-are-more-sophisticated-than-ever
3) Google Android Warning as Devious Spyware Hits the Play Store: www.forbes.com/sites/kateoflahertyuk/2019/08/22/google-android-spyware-warning-as-devious-app-hits-the-play-store-twice/
4) Russia bans sale of gadgets without Russian-made software: www.bbc.com/news/world-europe-50507849
5) 146 New Vulnerabilities All Come Preinstalled on [New] Android Phones: www.wired.com/story/146-bugs-preinstalled-android-phones/
6) An example of commercially available spy software: https://xnspy.com/features.html
7) Mysterious iOS Attack Changes Everything We Know About iPhone Hacking: www.wired.com/story/ios-attack-watering-hole-project-zero/
8) How an iPhone Vulnerability Allowed Websites to Hack iOS Devices: www.makeuseof.com/tag/how-websites-hacked-iphones/