CAB240 Information Security - Semester 2 2017
Mobile Phone Security Investigation Report
Part I - Task Requirements

This task is an investigation of information security issues associated with your personal mobile phone. Your report on the investigation will have two related parts. The focus in:

- **Part I** is examining your phone and your use of it, to identify relevant information security threats and vulnerabilities and identify risks.
- **Part II** is countermeasures to mitigate the risks you identified in Part I. Details on the report requirements for Part II form a separate document.

NOTE: If you do not have a mobile phone, you may complete this task for another mobile device. In that case, confirm suitability of your choice with unit coordinator before proceeding.

PART I Task requirements (and page length guidelines):
Your report should consist of the following sections:

1. A *brief description of the information assets* – what does your phone have? (2 pages)
    a. hardware – chipset, memory, screen , cameras, battery, communication components (you can find this information on a vendor specification page)
    b. software – operating system and applications (preloaded and those you installed),
    c. data – type and approx. volume of data you have stored (contacts, music, photos, etc)

2. An *overview of your use of the device* (1 page)
    a. note the sensitivity, criticality and importance of the particular assets that you described in Section 1 (relate to CIA goals),
    b. identify the applications you use most frequently, and those which are rarely used.

3. A summary of the *privacy policy for an app you use frequently*, (1-2 pages) including:
    a. what sort of information the app collects,
    b. how the information is collected,
    c. how the information is used by the app providers,
    d. how long collected information is stored for, and how and where it is stored,
    e. whether collected information is shared, and who it may be shared with,
    f. whether you (the app user) have access to the information held.

4. A summary of a *recent article identifying *a security issue associated with a mobile device application*, (1 page)
    a. if possible, find an article about an application that you use, or a widely used app.

5. A summary of a *recent article identifying *a security issue associated with a mobile device operating system* (operating system, not an application issue), (1 page)
    a. if possible, this should be for your phone operating system.

*recent article = publication date in 2017.

6. A summary of a *recent article identifying *a security issue associated with mobile device user behavior*, (1 page)
    a. focus on what the users do (or don't do) that causes the security issue.

7. A summary of a *recent article *identifying a physical threat to a mobile phone* (1 page)
    a. Lost or stolen phones are common, but there are others (e.g. flaming phones).

8. A *conclusion* relating the issues you have identified in your report to your personal information security (1 page).
    a. This should make connections between the points discussed in the earlier sections. Which assets are most at risk – what are the vulnerabilities and the threats that could exploit them? What would the impact be, and why is this important for you, as the device owner/user?

9. *Reference list*.

10. An *appendix* containing copies of the four articles you summarized (in Sections 4-7). Make it clear which section of your report relates to each article.

Academic writing
An important aspect of this assessment task is locating relevant information, either in online resources or in print media. However, your report should be in your own words. **Do not just 'cut and paste' or copy information from any source into the body of your report: that is plagiarism (a breach of academic integrity) and is not acceptable in Australian universities**. If a breach is detected, the Unit Coordinator must notify the Faculty Academic Integrity Committee, and the penalties imposed may be severe (See QUT MOPP for details). **In previous years, students have failed this unit as a result of the applied penalty.**
A useful guide to referencing, citation and report writing is: http://www.citewrite.qut.edu.au/ . QUT librarians will also provide assistance; check the QUT Library homepage for links.

Your report appendix will contain copies of the four recent mobile device security articles you selected (for Sections 4-7 of your report). Including copies of the articles in the appendix of your report is not a breach of academic integrity, as you are clearly acknowledging these articles as the works of other authors. The inclusion helps the markers process the very many student submissions we receive in a timely manner. If your article is long and the details you refer to in your summary are in the first page or so, include only the relevant section.

Report presentation
Please include the CAB240 unit code and your name and student number in the header or footer of each page. Use 12 point sized font.

Report submission
Electronic submission of a single file is via the Turnitin link on the CAB240 blackboard site. Under QUT's current Late Assessment policy, late submissions without an approved extension will receive a mark of 0 (so do submit before the deadline!).

*recent article = publication date in 2017.