CAB240 Information Security
Semester 2 2016

Mobile Security Investigation

This task is an investigation of information security issues associated with your personal mobile device – smartphone or tablet. Your report on the investigation will be completed in two parts.

PART I, consisting of:

1. a *brief description of the information security assets* (hardware, software – operating system and applications, data – type and approx. volume),
2. an *overview of your use of the device*, noting the sensitivity, criticality and importance of particular assets described above,
3. a summary of an article identifying *a security issue associated with a mobile device operating system*,
4. a summary of an article identifying *a security issue associated with a mobile device application*,
5. a summary of an article identifying *a security issue associated with mobile device user behavior*,
6. a *conclusion* relating the identified issues to your personal information security.
7. an *appendix* containing copies of the three articles you have summarized.

You should write approximately one page for each item 1-6. Your appendix will contain copies of the three mobile security articles you have selected. These articles should be recent (= publication date after May 2016).

For each of the three articles you select, the summary should be your own individual work, and written in your own words. Use the following template for items 3, 4 and 5:

Article summary template

Title: Article title
Author: Person, or organization if person not listed
Reference details (if online article, give URL and date accessed): Use the QUT library Cite|Write guide to see what is required for various sources. There's a link to this on the CAB240 Blackboard assessment page, and Cite|Write is also available at http://www.citewrite.qut.edu.au/
Brief summary: Give a really brief summary, just one short paragraph. However, it is important that you write this in your own words, not cut and paste from your article or copied from a friend. Penalties may be applied where copying is detected. In past years students have failed this unit as a result of the applied penalty.
Information asset: Which information assets are involved? What state is the information in?
Threat and / or vulnerability: Explain the threat. Categorize with respect to the threat source and type. Which security goal can be compromised (think CIA)? Explain the vulnerability. Categorize with respect to people/property/process.
Security incident / attack: Does the article describe a security incident or more specifically an attack? If an attack, explain how this works and categorize (passive/active, type). Is the attack being conducted in the wild (outside of research labs), or is it theoretical? How significant is the impact?

PART II of the investigation focusses on possible control measures to deal with the issues you have identified in this report. Details on the report requirements for PART II will be given in a separate document.