



HIGHER EDUCATION PROGRAMMES

| | |
|-------------------------|---|
| Academic Year 2023: | July - December |
| Summative Assessment 2: | Technical Systems and Support (HTSS100-1) |
| NQF Level, Credit: | 5, 24 |
| Weighting: | 10% |
| Assessment Type: | Research Essay |
| Educator: | L. Carolus |
| Examiner: | L Carolus |
| Due Date | 20 November 2023 |
| Total | 20 Marks |

Instructions

1. Summative Assessment 2 (SA 2) must be handed in online before or on the day of the Summative Assessment 1 (SA 1) sitting.
2. The essay must be a minimum of 500 (five hundred) words, and should not exceed 650 (six hundred and fifty) words.
3. The essay structure must be as follows:

- Cover Page:
 - Name
 - Surname
 - Student Number
 - Name of your Support Centre (i.e. Boston, Braamfontein)
- Introduction: Tells the reader what the essay is about.
- Body / Main Content: Is based on research and relates to the essay question or topic that has been set.
- Conclusion: Is a summary of what has been covered in the essay, it may also include suggestions / recommendations.
- Reference list: (not included in the word count): the Harvard Referencing Method must be adhered to with regards to in-text citations and the reference list. Please make sure you have read and adhere to the *NWU Referencing Guide*, available in the HE Library module on ColCampus, as well as *The Beginners Guide to Plagiarism*, available in the HE Student Information module, also on ColCampus.

4. The essay must be typed, using the following format settings only:

- Font: Arial
- Font Size: 12
- Line Spacing: 1.5

5. The following must be adhered to:

- ***You have been provided with one (1) academic source (see below), this source is compulsory and must be consulted and referenced when answering the research question.***
- ***It is imperative to note that the compulsory source must be accessed using the Library module on ColCampus.***

Compulsory source to peruse:

Skovoroda, A. and Gamayunov, D. (2016) "Securing mobile devices: malware mitigation methods," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 6(2), pp. 78–97. Retrieved from: <https://isyou.info/jowua/papers/jowua-v6n2-5.pdf>. [Accessed 6 March 2023].

6. You must make use of the Harvard Method of Referencing. Refer to the examples of referencing below:

Book, single author:

Holt, D.H. 2017. Management principles and practices. Sydney: Prentice-Hall.

Book, 2 or 3 authors:

McCarthy, E.J., William, D.P. & Pascale, G.Q. 2017. Basic marketing, Cape Town: Juta.

Book, more than 3 authors:

Bond, W.R., Smith, J.T., Brown, K.L. & George, M. 2016. Management of small firms, Sydney: McGraw-Hill.

Book, no author:

Anon. 2009. A history of Greece 1994-now. Sydney: Irwin.

eBook:

Harris, C.A. 1917. How to write music: musical orthography, edited by M. Randall. New York, NY: H. W. Grey. <http://gutenberg.org/files/37281/37281-h/37281-h.htm>. Date of access: 31 August 2017.

Academic Journal article with one author:

Allan, J. 2017. Nurturing supportive learning environment in higher education through the teaching of study skills: to embed or not to embed? *International Journal of Teaching and Learning in Higher Education*, 19(2):64-76.

Academic Journal with 2 or more authors:

Glatt, M.M., Grindstone, C.H & Hult, C.J. 2019. The geographic expansion of Mexican immigration in the United States and its implications for local law enforcement. *Law Enforcement Executive Forum Journal*, 8(1):73-82.

Webpage, no author:

(use first few words of the page title) Improve indigenous housing now, government told. 2007. Available from: <<http://www.architecture.com.au/i-cms?page=10220>>. Date of Access, 8 February 2016.

Website:

Australian Securities Exchange. 2019. Market Information. Available from: <http://www.asx.com.au/professionals/market_information/index.htm> Accessed on 5 July 2019.

Web based image / table / figure:

The Lunar Interior. 2000. Available from: <http://www.planetscapes.com/solar/browse/moon/moonint.jpg> 2 Accessed on 8 November 2016.

Blog:

Newton, A. 2007. Newcastle toolkit. 16 January 2007. Angela Newton: Blog. Available from: <<https://elgg.leeds.ac.uk/libajn/weblog/>> Accessed on 23 February 2014.

Facebook and Twitter:

Smith, P. 2012. Social networking group, (Facebook), 6 October. Available from: <http://facebook.com> Accessed on 29 October 2012.

Newspaper, print:

Wolhuter, T. 2011. How to read food labels. *Star*. 26, 2 Mar 2011.

Newspaper, electronic database:

Hans, B. 2011. Cosatu slams Swazi loan. *The mercury*, 15 Aug. <http://www.iol.co.za/mercury/cosatu-slams-swazi-loan-1.1117816> Date of access: 1 Sep. 2012.

7. Plagiarism occurs when a writer duplicates another writer's language or ideas, and then calls the work his or her own. Simply put, plagiarism is theft. This includes the 'copy and paste' of work from textbooks, study guides, journal articles. The Plagiarism Declaration, included in this brief, must be signed and attached to the front of your essay. Refer to the Plagiarism Information Sheet in your Course Outline for further information.

8. **Academic sources:**

Not all sources can be classified as an academic source. To judge whether a source is an academic source, take the following criteria into account:

- The author should be identifiable
- The source should be published by a credible publisher (In an Academic Textbook or Academic Journal)
- A list of references should be provided

Wikipedia **is not** a credible academic source. There is no author identifiable, and editing an article on this site is very easy. Also, blog posts often provide valuable information, but this is not academically sound.

9. To obtain maximum results, please consult the rubric included in this brief to ensure that you adhere to and meet all the given criteria.

10. A **Copyleaks Report** will be issued via ColCampus once the assignment is submitted. Please ensure that you follow the correct steps when uploading your assignment, to ensure that the Copyleaks Report is correctly issued. If the incorrect document is uploaded, or if no Copyleaks Report is issued, a mark of zero (0) will be awarded. If the Copyleaks Report indicates that a 30% similarity rating has been exceeded, 25% of the assessment total will be deducted from the final grade. Where a Copyleaks Cheat Detection Report is issued, your submission will automatically be treated as if you received a similarity rating in excess of 30% and 25% of the assessment total will be deducted from the final grade.

Question 1

(20 Marks)

From the simple task of sending and replying to emails, to handling business finances the use of mobile handsets for business tasks has grown much in the past decade. With the usage growth comes the increased risk of security breaches within an organisation (Skovoroda & Gamayunov, 2016). Therefore, as an IT technician in today's age, you must be well-versed in mobile device security and the risk of information breaches caused by malicious content.

In this paper, you are required to research different types of malware that can affect mobile devices, their detection methods, and treatment and prevention methods.

Compulsory source to peruse:

Skovoroda, A. and Gamayunov, D. (2016) "Securing mobile devices: malware mitigation methods," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 6(2), pp. 78–97. Retrieved from: <https://isyou.info/jowua/papers/jowua-v6n2-5.pdf>. [Accessed 6 March 2023].

The following Learning Outcomes are assessed in this assessment:

Elaborate on Green computing.

| Criteria | Exceptional | Satisfactory | Developing | Unsatisfactory | Total |
|---|--|--|---|--|------------|
| Examine mobile device malware threats, detection methods, and treatment and prevention methods. | Student has comprehensively explained atleast: <ul style="list-style-type: none"> Malware threat types (5) Detection methods (7) Prevention and treatment methods (5) | Student has sufficiently explained Mobile device: <ul style="list-style-type: none"> Malware threat types Detection methods Prevention and treatment methods | Student has merely outlined mobile device: <ul style="list-style-type: none"> Malware threat type Detection methods Prevention and treatment methods | Insufficient explanation of Mobile device: <ul style="list-style-type: none"> Malware threat types Detection methods Prevention and treatment methods | |
| | 17-14 | 13-10 | 9-5 | 4-0 | |
| Bibliography and References | Exceeds the number of relevant sources (2+). Compulsory source consulted | Minimum relevant sources met. Correct Harvard referencing | Some sources were quoted, but irrelevant. Incorrect referencing | None | |
| | 3 | 2 | 1 | 0 | /20 |