**QUESTION 2.**

**Ethics:** The values and concepts that help people and organizations decide what is good or evil, fair or unfair, and right or wrong in their activities are referred to as ethics. It entails making choices with the common good, other people's welfare, and the harmony of rights and obligations in mind. Ethical behavior in the workplace necessitates upholding moral principles of justice, honesty, and integrity.

Ethics is centered on well-established moral principles that dictate what people should do, typically in terms of rights, duties, societal advantages, justice, or qualities. (University, n.d.)

1. **Hacking into the system:** computer hacking is broadly defined as intentionally accessing a computer without authorization or with exceeding authorized access.(Cekerevac et al., 2018).

**Ethical Approach:** It is a breach of privacy and trust to access someone else's system without authorization. Rather, the individual ought to adhere to privacy and data ownership regulations. To help improve security without abusing it, people should report vulnerabilities through the proper channels, such as a vulnerability disclosure program, if there are security concerns.

2. **Plagiarism of software development:** The word originates from the Latin *“plagiarius”*, meaning torturer, oppressor, or kidnapper.(Folea & Slusanschi, 2024)  
To finish a project or assignment, a developer steals software or code from someone else and passes it off as their own.

**Ethical Approach:** Respecting intellectual property by correctly identifying and recognizing the original developer of the software or code is the ethical method to go about this. The developer should adhere to attribution guidelines and license agreements when reusing open-source software.

3. **The development of malicious software, or malware:** Malicious software, or malware for short, is software designed with the nefarious intent of harming the computer user. (Ngo et al., 2020).

**Ethical Approach:** Software should not be created to harm or exploit people, but rather to address problems, increase security, or enhance user experiences. Using their expertise for good, such as creating security tools or ethical hacking software that assists corporations in identifying and patching holes to safeguard users, would be a more moral choice for such a coder.

**REFERENCES:**

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2018). HACKING, PROTECTION AND THE CONSEQUENCES OF HACKING. *Komunikácie*, *20*(2), 83–87. https://doi.org/10.26552/com.c.2018.2.83-87

Folea, R., & Slusanschi, E. (2024). On Plagiarism and Software Plagiarism. In N.-T. Nguyen, B. Franczyk, A. Ludwig, M. Nunez, J. Treur, G. Vossen, & A. Kozierkiewicz (Eds.), *Advances in Computational Collective Intelligence* (pp. 314–326). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70259-4\_24

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious Software Threats. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 793–813). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3\_35

University, S. C. (n.d.). *What is Ethics?* Retrieved October 24, 2024, from https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/what-is-ethics/