

1. Pokémon Go is a free-to-play, location-based augmented reality game. Answer the following questions on the subject based on the newspaper article link below. <https://www.malaymail.com/s/1180221/pokemon-go-carries-same-security-risks-as-other-mobile-apps-says-it-expert>
2. Based on the article, explain how the Pokémon Go game can potentially affect the security objectives of its users, namely the confidentiality, integrity and availability. Explain through suitable examples of the potential risk faced by each objective and how to make it secure.

(12 Marks)

1. Does personal data need to be protected? Give 3 reasons to support your answer.

(6 Marks)

1. The PDPA (Personal Data Protection Act 2010) regulates how personal data can be collected, processed and used in Malaysia. With such an Act, should users in Malaysia be concerned? Explain your answer by giving appropriate examples.

(4 Marks)

1. In your opinion, should the Pokémon Go game be banned? Justify your answer.

(4 Marks)

1. What are the available methods of precautions that game and app users like Pokémon Go can take to mitigate the risks?

(4 Marks)



<https://www.financialexpress.com/opinion/whatsapp-hack-shows-how-supposedly-secure-messaging-apps-have-a-basic-vulnerability/1579413/>

1. The above article highlights on the discovery of how hackers could snoop on WhatsApp would alert users of supposedly secure messaging apps to an uncomfortable truth: “End-to-end encryption” sounds nice — but if anyone can get into your phone’s operating system, they will be able to read your messages without having to decrypt them.
2. Explain what is an “End-to-end encryption” and how does it help to secure communication?

(4 Marks)

1. There have been suggestions to create an encryption backdoor, to let the government stop “Bad Things” and does sounds like a reasonable idea. Do you agree or disagree that the government should be allowed to have an encryption backdoor? Give three reasons to support your answer.

(10 Marks)

1. Taking WhatsApp as an example, is it technically feasible to have an encryption backdoor for an “End-to-end encryption” system? Explain your answer by giving an example of an “End-to-end encryption” between a sender, Alice with a receiver, Bob using a shared key Kab.

(10 Marks)

1. “*The malware could access a phone’s camera and microphone, open messages, capture what appears on a user’s screen, and log keystrokes — rendering encryption pointless.*”
2. Based on the above quote from the article, is “End-to-end encryption” a pointless process to secure a communication channel? Do you agree with the statement? Give two reasons to support your answer.

(6 Marks)