**Quiz 5.1**

**Michael Christopher – s224830467**

1. **Developing an AI system that generates someone's video face to fool a face recognition system of a phone.**

   This situation shows an impersonation assault using deepfake technology enabled by AI. Here, artificial intelligence is being used maliciously to produce a realistic-looking fake video of a person's face that can get past biometric identification systems like smartphone facial recognition. This technique uses advanced generative models, including Generative Adversarial Networks (GANs), to create dynamic, realistic face motions, which makes it far more difficult for the recognition system to identify fraud than typical spoofing techniques (like holding up a photo).

   The justification is that deepfake-based impersonation challenges the idea that biometric systems rely on distinctive human characteristics for safe authentication by synthetically mimicking such characteristics. Very serious consequences might result from identity fraud, financial theft, or illegal access to private information. Furthermore, this illustrates the larger problem of AI being used maliciously, as technologies intended for amusement or creativity are used to launch cyberattacks.

2. **Developing an AI system to talk/chat as a person to collect information from his colleagues on a company cyber protection system.**

   This situation depicts social engineering via impersonation made possible by AI. To fool people, it involves creating an artificial intelligence (AI) system that can realistically replicate a person's communication style. This system is probably built on Natural Language Processing (NLP) and big language models. Tricking coworkers into disclosing private information about the organization's cyber defences is the malicious aim, which might then be used to launch more assaults.

   Because conventional phishing and social engineering rely on human attackers creating false communications, this categorization is justified. Here, AI creates context-aware, human-like dialogues, which expands the attack's scope, complexity, and realism. By posing as a reliable insider, the AI gets past many of the targets' psychological barriers, leading them to think they are interacting with a genuine coworker.

3. **Developing an AI system to identify users susceptible to click on a malicious link.**

   This situation shows targeted exploitation and phishing with AI assistance. To identify the people who are most susceptible to manipulation, the AI system is being used to examine user behaviour, online activity, or digital communication patterns. Once located, attackers can target these high-risk consumers with malicious links or phishing operations, improving the chances of success.

   The justification is because classic phishing frequently uses broadcasting or mass emailing in the hopes that a few individuals would fall for the trick. AI, on the other hand, adds accuracy by profiling people according to their prior interactions, linguistic clues, emotional states, and browsing patterns. This turns phishing from a broad assault into spear-phishing, a customized, extremely focused tactic.

   The consequences for security and ethics are serious. Attackers may now deliver dangerous material more easily thanks to AI, which also helps them carefully take advantage of human flaws, making defences considerably more difficult. This abuse is a prime example of the larger category of malicious AI in cybercrime, where AI automates surveillance and personalized deception to increase the effectiveness of traditional attack techniques.

4. **Developing an AI system to identify users susceptible to share banking information – for instance credit card number.**

   This situation shows social engineering-based financial exploitation powered by AI. Maliciously, the AI system is being used to identify those who are more prone to share private banking information, such credit card numbers, when pressured or persuaded. AI is used in this situation as a tool to methodically take advantage of psychological weaknesses by predicting sensitivity through the analysis of behavioural characteristics, communication styles, or even demographic data.

   The justification is that conventional scams frequently cast a wide net and hope that a small number of victims would react. Attackers may use AI to improve this process by identifying those who are most likely to fall for scams using data analysis and predictive modelling, significantly boosting efficiency and success rates. Under the pretence of phishing, vishing (voice phishing), or fake customer service contacts, this turns opportunistic fraud into a precisely targeted financial attack.

   The consequences are severe as it reduces confidence in digital communications and financial systems in addition to raising the possibility of direct financial theft. This type of hostile AI is a serious ethical transgression, demonstrating how AI, when used as a weapon, increases the scope and accuracy of human deception and reduces the effectiveness of conventional countermeasures.