Task 1

1. Intrusive application practices : Applications that collect more data than actually required, or the misuse of permissions, may pose a risk to user privacy .

2.Account credential theft through phishing : The attacker tricks the user into revealing his login credentials by sending fake emails, websites, or messages supposedly from genuine sources that looks identical to some other pages or website .

3.Outdated phones: Phones not updated with state-of-the-art patches are highly vulnerable to malware, exploits, and security breaches .

4.Sensitive data transmissions: Passwords and financial data, which are usually sensitive, are easily intercepted when transmitted over an unsecured network .

5.Brute-force attacks to unlock a phone : The hackers make repeated gueses with multiple password combinations until they finally unlock the phone, especially in cases where poor security measures are implemented .

6.Application credential storage vulnerability: Poorly designed credential storage by an app will lead to them getting easily stolen by an attacker or malware.

7. Unmanaged device protection : The data that is susceptible to being affected by leakage resulting from some unmanaged , out-of-control devices that the IT departments cannot manage , such as personal phones .

8.Lost or stolen data protection: Making sure even the most sensitive data remains secure even , when the device is stolen or lost thanks to encryption or remote wiping .

9.Protecting enterprise data from being inadvertently backed up to a cloud service : Corporate sensitive data does not get backed up automatically to personal or unauthorized cloud services where security is weaker .