# week 5 task 1

- Intrusive application practices mean ways to lure sensitive information or other sensitive data from a user through an application or application download. For example in the pdf document there is an example of Unauthorized access to work information via a malicious or privacy-intrusive application.

- malicious actors can create websites that mimic other websites or otherwise seem trustable and lure users to authenticate in them by for example distributing phishing messages to the users. When users authenticate, their credentials are captured

- malicious actors can eavesdrop unprotected networks and gain access to users sensitive data while they are transmitting it. Example of these would be public Wifi networks. Even if the transmissions are encrypted there is still a slight chance of eavesdropping.

- Brute-force attacks to unlock a phone work so that the malicious actor might be able to gain access to the users device through obtaining their device's unlock code with brute force attacks that go through the different possible unlock codes with trial and error.

- Application credential storage vulnerabilities occur when there is no proper and essential protection for passwords. These have many examples but some are failure of encrypting password data, store the credentials in a file that is easily accessible and hard coded passwords that are easily passable by the malicious actor.

- users who access some resources through unmanaged devices might expose the resources to threats. They usually are devices that for example employees own personally and when they access enterprise resources for example from an unmanaged mobile device, they put the enterprise at risk and expose it to threats.

- lost or stolen data are devices or resources that are either lost or stolen. for example a mobile device is so small that it is in risk or being stolen or being lost. A malicious actor who gains access to the lost device or other resource might be able to gain unauthorized access to the resources sensitive data.

- if for example employees use unmanaged services to store sensitive organizational data, the control of the data is outside of the organizations control and it can no longer be protected. If malicious actors gain access to these unmanaged services, they might gain unauthorized access to the data. It is important to use protected and managed services that the organization can control to store sensitive data.