intrusive application practices

- Apps installed on personal phones that excessively collect data without clear authorization (compromising user privacy and company data security).

Account credential left through phishing

- Malicious people try to steal your login via fraudulent messages, emails or website

Unmanaged device protection

In a company, personal devices that are not monitored by its policies may not have adequate protection against outside threats.

outdated phones

old phones that are no longer updated are vulnerable to known vulnerabilities that cybercriminals can exploit

sensitive data transmissions:

sending sensitive data over unsecured channels (ex: public wifi) exposes you to the risk or information theft.

Brut-force attacks to unlock a phone:

When a personnal phone is lost or stolen, an attacker can attempt to unlock the device by trying a large number of combinations - until finding the correct one.

Application credential storage Vulnerability

Some applications do not store authentification information correctly.
An attacker can access user accounts.

lost or stolen data protection

If a personal device containing corporate data is lost or stolen, mechanisms such as encryption and remote control must be in place to prevent exposure of sensitive information

Protecting enterprise data from being inadvertently back up to a cloud service

Corporate data can be automatically backup up to the user's personal cloud, compromising information security, especially if the service is not secure