移動網絡是指基於移動通信技術，提供移動通信服務的無線通信網絡；而移動網絡及其安全問題是指移動通信網絡和移動終端設備在傳輸和處理數據時可能遇到的各種威脅和風險，常見的威脅和風險包括：

1.) 竊聽和監聽：攻擊者通過竊聽和監聽網絡流量，獲取用戶的敏感信息，如帳號、密碼、個人信息等。

2.) 欺騙：通過虛假或欺騙性信息來欺騙使用者，讓他們相信所提供的服務或產品是真實可信的，從而讓用戶洩露敏感信息或執行惡意操作。網路欺騙的形式包括假冒網站、仿冒身份、假冒網絡服務、虛假廣告、詐騙郵件等等。

3.) Signaling Hijacking 通訊劫持：包括「手機通訊劫持」、「行動電話劫持」、「基地台劫持」、「移動通訊窃聽」等，攻擊者利用網絡漏洞或者其他方式，篡改或者竊取移動網絡的信令數據，從而實現窃聽、跟蹤、偽造、劫持等攻擊，導致用戶無法正常連接到移動網絡，或者將用戶連接到惡意的網絡。

4.) 惡意軟件：指具有破壞性、欺騙性或其他危害性的電腦程式，在未經用戶授權的情況下安裝在用戶的電腦上，並進行一系列惡意活動。惡意軟件可以有多種形式，包括病毒、蠕蟲、木馬、間諜軟件、廣告軟件和勒索軟件等。惡意軟件甚至還將用戶的電腦變成僵屍網絡的一部分、攻擊其他電腦系統、刪除或加密用戶的文件等。

為了保障移動網絡的安全，需要採取一系列的安全措施，包括：

1.) 定期更新作業系統和應用程式，以修補已知的漏洞和強化安全性。

2.) 使用可靠的防毒軟體和防火牆，並且定期更新，以阻止惡意軟體和攻擊的入侵。

3.) 避免使用不明來源的連接埠、甚至公共Wi-Fi ，以防止網路竊聽或中間人攻擊。

4.) 設定密碼、指紋或臉部辨識等鎖定方式，以防止未經授權的存取。

5.) 備份重要資料，以防止資料遺失或毀損。

6.) 為了保護個人隱私和防止電腦系統被惡意軟件攻擊，不隨意下載和安裝未知的軟件、不點擊可疑的郵件附件或網頁鏈接，以及不在不安全的網站上輸入個人信息。

7.) 此外，網絡運營商和政府也需要加強對移動網絡的監管和管理，以保障用戶的安全和權益。

在移動互聯網快速發展的當今，移動網絡安全問題已經成為不容忽視的議題。為了保障移動網絡的安全，需要廣泛管理措施，包括加強對移動網絡的監管、提高用戶的安全意識、開發更加安全可靠的移動應用程序等等。只有全面的加強移動網絡的安全保障，才能讓移動互聯網更好地發展。