Connecting your world.

Telekom **MobileSecurity**

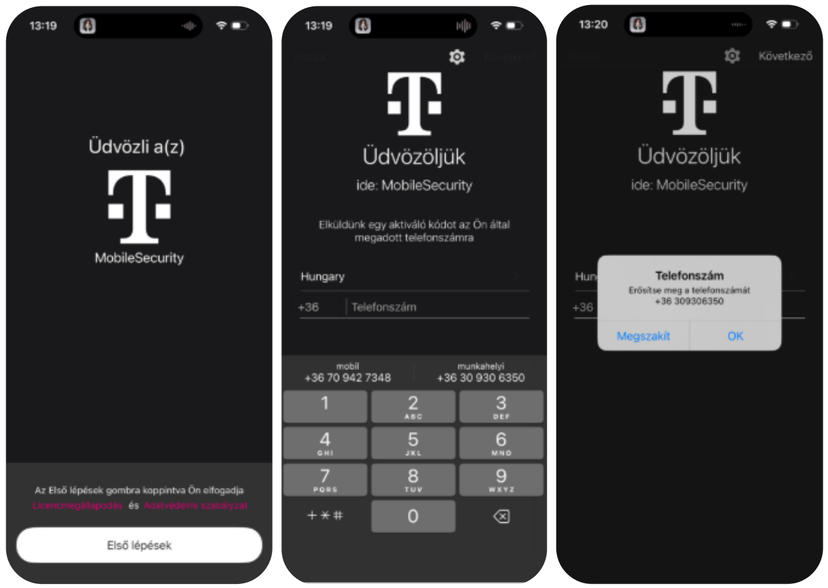
A Telekom MobileSecurity egy átfogó mobilbiztonsági megoldás, amelyet a Check Point ZoneAlarm technológiájára építve fejlesztettek ki. Célja, hogy a felhasználók mobil eszközeit (okostelefonok, tabletek) megvédje a folyamatosan fejlődő kiberfenyegetésekkel szemben, legyen szó hálózati, alkalmazás- vagy eszközszintű támadásokról.

Connecting your world.

Regisztráció és Beállítások

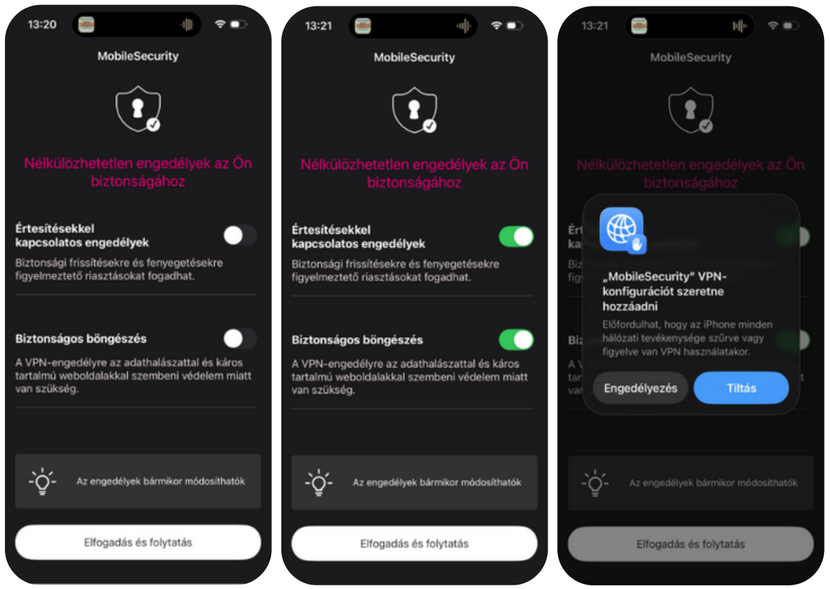
1. Üdvözlőképernyő és Aktiválás:

Az alkalmazás indításakor egy üdvözlőképernyő fogadja a felhasználót, ahol a "Első Lépések" gombra kattintva kezdődik a folyamat. Ezt követően a rendszer egy aktiváló kódot küld a megadott telefonszámra, amelyet be kell írni az alkalmazásba.



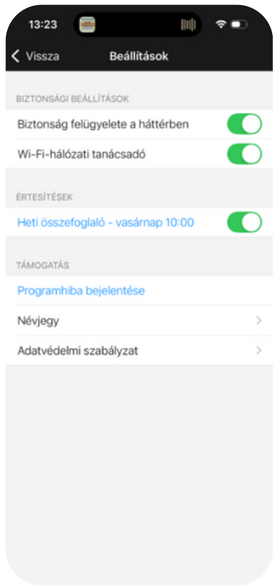
2. Alapvető Engedélyek

A biztonsági funkciók teljes körű működéséhez az alkalmazás alapvető engedélyeket kér, mint például az értesítések fogadása és a Biztonságos Böngészés funkcióhoz szükséges VPN kapcsolat beállítása. Fontos, hogy ezeket az engedélyeket megadjuk a maximális védelem érdekében.



3. Személyre Szabható Beállítások

A felhasználók testre szabhatják a biztonsági beállításokat. A "Biztonsági Beállítások" menüpontban beállítható a háttérben futó biztonsági ellenőrzés ("Biztonsági felügyelet a háttérben") és a Wi-Fi hálózati tanácsadó aktiválása. Emellett heti összefoglaló értesítések is kérhetők.



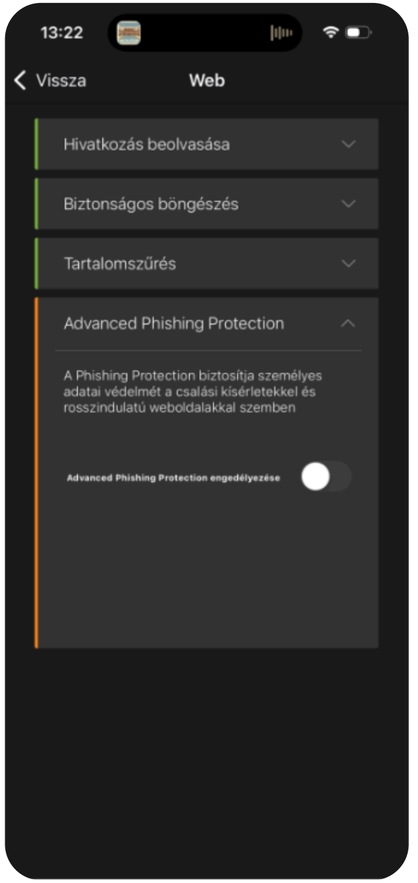
Connecting your world.

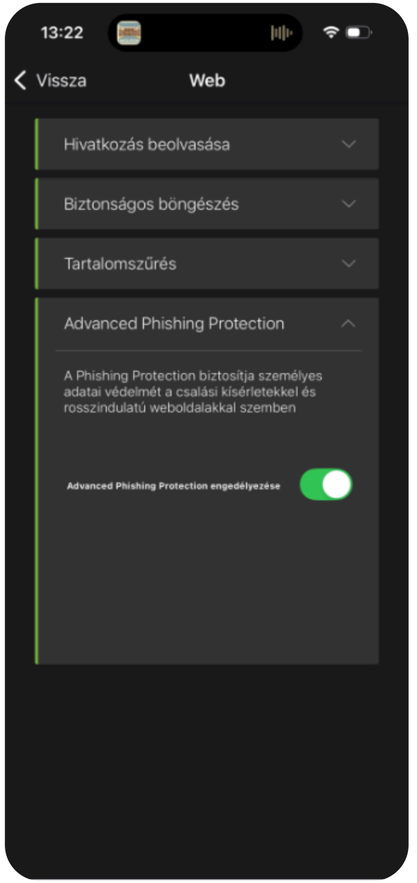
Biztonsági Funkciók Részletesen

A Telekom MobileSecurity számos fejlett biztonsági funkciót kínál, amelyek a Check Point ThreatCloud AI alapjaira épülnek, valós idejű fenyegetésfelderítést és -elhárítást biztosítva.

1. Phishing Szűrés (Zero-Phishing és Advanced Anti-Phishing

- **Valós idejű védelem:** Az alkalmazás valós időben ellenőrzi az összes meglátogatott weboldalt és a QR-kódokon keresztül elérhető linkeket. Ha egy weboldal vagy link rosszindulatúnak minősül (pl. adathalász oldal), azonnal blokkolja azt, megakadályozva a felhasználó érzékeny adatainak (pl. bankkártya adatok, bejelentkezési adatok) ellopását.
- **Zero-day védelem:** Képes felismerni és blokkolni az eddig ismeretlen, ún. "zero-day" adathalász támadásokat is, amelyek a hagyományos védelmi rendszereken könnyedén átjuthatnának.
- **QR-kód alapú adathalászat (Quishing) elleni védelem:** A QR-kódok egyre gyakoribbak, és a támadók előszeretettel használják őket rosszindulatú weboldalakra mutató linkek elrejtésére. Az alkalmazás QR-kód szkenner funkciója lehetővé teszi a kódok biztonsági ellenőrzését, mielőtt a felhasználó megnyitná a mögötte rejlő tartalmat.





Connecting your world.

Biztonsági Funkciók Részletesen

A Telekom MobileSecurity számos fejlett biztonsági funkciót kínál, amelyek a Check Point ThreatCloud AI alapjaira épülnek, valós idejű fenyegetésfelderítést és -elhárítást biztosítva.

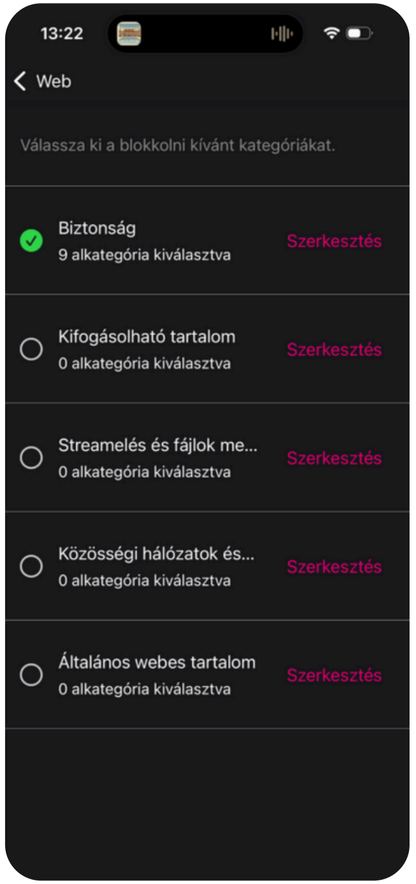
2. Forgalom Szűrés és Hálózati Védelem

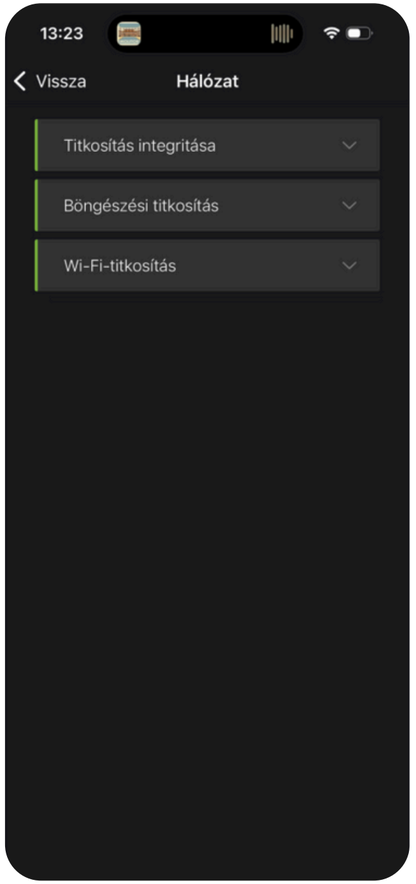
- **On-Device Network Protection (ONP):** Ez a technológia az eszközön belül validálja az összes felhasználói forgalmat anélkül, hogy az adatokat a felhőbe irányítaná. Ez garantálja az adatvédelem magas szintjét, miközben zökkenőmentes böngészési élményt és minimális akkumulátorhasználatot biztosít.

- **Eavesdropping Protection (Lehallgatás elleni védelem):** Megvédi a felhasználót a Man-in-the-Middle (MitM) támadásoktól, különösen nyilvános Wi-Fi hálózatokon. Ellenőrzi az SSL/TLS kapcsolatok integritását, és figyelmeztet, ha a hálózat kompromittált.

- **Wi-Fi Hálózati Biztonság:** Értékeli a rendelkezésre álló Wi-Fi hálózatok biztonsági szintjét, és segít a felhasználónak a legbiztonságosabb opció kiválasztásában. Figyelmeztet a nem biztonságos Wi-Fi kapcsolatokra.

- **Tartalomszűrés (Content Filtering):** Lehetővé teszi a felhasználó számára, hogy blokkolja a nem megfelelőnek ítélt webes tartalmakat kategóriák alapján (pl. streaming és fájlmegosztás, nem megfelelő tartalom, közösségi média és játék, rosszindulatú weboldalak). Ez különösen hasznos lehet családi környezetben vagy vállalati szabályzatok betartatására.





Connecting your world.

Biztonsági Funkciók Részletesen

A Telekom MobileSecurity számos fejlett biztonsági funkciót kínál, amelyek a Check Point ThreatCloud AI alapjaira épülnek, valós idejű fenyegetésfelderítést és -elhárítást biztosítva.

3. Egyéb Fontos Biztonsági Funkciók

- **Alkalmazásvédelem (App Protection - Android):** Megvédi az eszközt az ismert és ismeretlen rosszindulatú alkalmazásoktól és frissítésektől. Az alkalmazásokat egy felhőalapú környezetben (Behavioral Risk Engine - BRE) elemzi, amely gépi tanulást és AI-t használ a fenyegetések azonosítására.
- **Eszközvédelem (Device Shield):** Figyelmeztet a kockázatos eszközkonfigurációkra, például a harmadik féltől származó alkalmazások telepítésének engedélyezésére. Érzékeli a rootolt/jailbreakelt eszközöket, és figyelmeztet, ha valaki jogosulatlanul hozzáfér az operációs rendszerhez.
- **Adatlopás elleni védelem (Data Leakage Protection):** Blokkolja az érzékeny adatok kiszivárgását a rosszindulatú kommunikációkon keresztül.
- **Zero-day Ransomware Protection:** Gépi tanulási képességeket használ az ismert és ismeretlen zsarolóvírus-támadások blokkolására, és képes visszaállítani a titkosított fájlokat.
- **Biztonságos Letöltések (Secure Downloads):** Semleges környezetben vizsgálja a letöltött fájlokat a potenciális fenyegetések szempontjából, mielőtt azok elérnék a felhasználó számítógépét.
- **Heti Személyre Szabott Jelentések:** Az eszközön generált heti biztonsági incidensjelentések tájékoztatják a felhasználót a legújabb fenyegetésekről, amelyeket a Telekom MobileSecurity sikeresen elhárított.