Biztonsági beállítások

Sziasztok! Folytatjuk a Mosaic OS operációs rendszer bemutatását. A hangsúly továbbra is a biztonságon, az adataink védelmén van, ezt szolgálja a Pixel telefonokban lévő Titan M2 chip is, amely hardveres biztonságot ad, nehezíti a szoftveres, jogosulatlan manipulációt, és a fizikai támadásokat is. Néhány beállítással azonban tovább fokozhatjuk a biztonságot. Alapvetően mindenkinél máshol van az a határ, ahol a kényelmet választja a biztonság rovására, vagy adott esetben fordítva, a biztonságot választja a kényelem rovására. Ezek a beállítási lehetőségek nem azt jelentik, hogyha akár egyet is kihagyunk, és nem úgy használjuk, ahogy a nagy könyvben meg van írva, akkor már nem is biztonságos a telefon. DE! A Mosaic OS már az alapbeállításokkal is sokkal nagyobb biztonságot nyújt, mint a mai legnépszerűbb operációs rendszerek, ezekkel a plusz beállításokkal csak tovább fokozhatjuk az adataink védelmét. Mindenki eldöntheti, hogy melyik opció az, aminek használata még kényelmes. Ezeket mutatjuk most be:

1. A nyílt hálózatokat lehetőleg kerüljük, automatikusan ne engedjük a telefonunknak, hogy nyílt hálózathoz csatlakozzon. **Először menj a Beállítások → Hálózat és internet → Internet** menübe, görgess le a **Hálózati beállítások** részhez. Győződj meg róla, hogy a **Wi-Fi automatikus bekapcsolása** ki van kapcsolva – soha nem akarod, hogy a Wi-Fi magától bekapcsoljon és jeleket küldjön bárhol, bármikor. Az **Értesítés a nyilvános hálózatokról** legyen kikapcsolva! **A WEP-hálózatok engedélyezését** sem javasoljuk használni, csak és kizárólag akkor használj WEP-es hálózatot, ha csak így tudsz internethez jutni. Minden más esetben kerülni kell, mert egy ilyen hálózat sebezhető, a megfelelő eszközökkel pár perc vagy óra alatt feltörhető a jelszó.
   A **Beállítások → Biztonság és adatvédelem → Kihasználás elleni védelem → Wi-Fi automatikus kikapcsolása** legyen időzítőre állítva; én 1 percet választok, ez azt jelenti, hogy ha elmegyek otthonról, és egy percig nincs Wi-Fi-kapcsolat, a telefon automatikusan kikapcsolja a Wi-Fi-t. Minél rövidebb időt választasz, annál jobb.
   Ha így használod a telefont, teljes mértékben neked, manuálisan kell beállítani, hogy épp Wi-Fi-t vagy mobil internetet szeretnél használni.

2. **Beállítások → Hálózat és internet → Hotspot és internetmegosztás → Wi-Fi hotspot**: amilyen gyakran csak lehet, tartsd a **Wi-Fi hotspot használata** opciót kikapcsolva. Ha mégis használnod kell, a **Hotspot neve** ne olyan legyen, amiről beazonosítható a személyed vagy a telefonod. Hiszen ez is nyilvános. A **Biztonság** opciónál mindig az eszközöd által támogatott legmagasabb titkosítást válaszd, soha ne a „nincs” lehetőséget. A **WPA2 és WPA3 protokoll** a jelszó titkosításáért felel. A WPA2 alatti protokollok már nagyon sebezhetőek, ezek már meg sem jelennek itt, a WPA3-at viszont még nem mindegyik eszköz támogatja. Így a legjobb a **WPA2/WPA3-Personal** lehetőséget választani, mert így azok az eszközök, amelyek támogatják a WPA3-at, ezzel fognak csatlakozni, amelyek nem, azok WPA2-vel. Állíts be erős **Hotspot jelszó**t. A **Wi-Fi-hotspot automatikus kikapcsolása** legyen kipipáva, így ha nincs csatlakoztatott eszköz, magától leáll a hotspot. Ha az **Adatforgalom-csökkentő** be van kapcsolva, nem lehet használni ezt a hotspotot.

3. **Beállítások → Hálózat és internet → Privát DNS**: állítsd **Automatikusra**! Amikor felkeresel egy weboldalt, átfut a kérésed egy DNS-szerveren. Ha privát DNS-t használsz, nem például a Google-ét, akkor nem a Google szerverén megy keresztül a

kérés, így nem látja majd ezt a tevékenységet a Google. Lehet különböző privát DNS-szolgáltatókat is használni, ha valaki még nagyobb biztonságot szeretne elérni, de egy átlag felhasználónak teljesen jó az **Automatikus** opció. A **Privát DNS-szolgáltató gazdagépneve** opciót akkor válaszd, ha privát DNS-szolgáltatót szeretnél használni. Az egyik legnépszerűbb ezek közül a Next DNS. Saját weboldalán keresztül a Next DNS feltünteti a használati utasításokat, ezt a folyamatot végigpörgetve kapsz egy címet, amit a **Privát DNS-szolgáltató gazdagépnevéhez** lehet beírni. Ez annyiban fokozza a biztonságot, hogy tiltja a reklámos és a rosszindulatú felületeket is.

4. **Beállítások → Hálózat és internet → VPN**: ezzel biztonságosabbá tehetők az online tevékenységek, egy titkosított alagutat hoz létre az internetkapcsolatod és a VPN-szolgáltató szervere között. Egy átlag felhasználónak nincs szüksége ilyenre.
5. **Beállítások → Hálózat és internet → Internetkapcsolat ellenőrzése**: alapértelmezetten **GrapheneOS szerver** – ezt hagyhatod, vagy kikapcsolhatod. Ennek annyi a lényege, hogy van-e az adott hálózatnak internetkapcsolata és min keresztül történik az ellenőrzés. A lényeg, hogy ne a **Standard (Google) szerver** legyen használva.
6. **Beállítások → Csatlakoztatott eszközök → Az összes megtekintése**: láthatod az összes mentett eszközt, mellettük a fogaskerékre koppintva kapcsold ki a felesleges engedélyeket.
7. **Beállítások → Csatlakoztatott eszközök → Kapcsolati beállítások → Bluetooth**: az **Eszköz neve** ne utaljon rád vagy a telefonodra, soha ne a saját nevedet add meg, hiszen ez is nyilvános információ.
8. **Beállítások → Csatlakoztatott eszközök → Kapcsolati beállítások → NFC**: ideiglenesen most kapcsold be a használatát, hogy hozzáférj a következő lehetőséghez: **Az NFC használatához fel kell oldani az eszköz zárolását**. Ezt pipáld ki. Utána kapcsold ki az **NFC használatát**. Ezt most azért csináltuk, mert általában az emberek bekapcsolva tartják az NFC-t, tehát zárolt kijelzőnél is működik az NFC-kommunikáció. Ez azért kényelmes, mert ha telefonnal fizetünk a boltban, csak odatartjuk a telefont a terminálhoz és kész is a fizetés. De ha valakinél van egy zsebterminál vagy egyéb eszköz, ami ugyanezt az NFC-kommunikációt tudja végrehajtani, akkor bárhol, bármikor a lezárt telefonod közelébe tartva az eszközt, már le is tudta emelni róla a pénzt. Mosaic OS-en Google Pay-vel nem lehet fizetni, de vannak olyan szolgáltatások, amelyek így is tudnak működni.
9. **Beállítások → Csatlakoztatott eszközök → Kapcsolati beállítások → Nyomtatás**: az Alapértelmezett nyomtatási szolgáltatás mindig legyen kikapcsolva.
10. Menj vissza a fő **Beállítások** oldalra, majd **Alkalmazások → Összes alkalmazás megtekintése**: minden alkalmazásnál nézd át a beállításokat, és tagadj meg minél több engedélyt. Ez időigényesebb beállítás, hiszen minden alkalmazásnál egyenként le lehet tiltani azokat a hozzáféréseket, amelyekre egyáltalán nincs szüksége a működéshez. Mindegyik alkalmazásnál van egy olyan lehetőség, hogy **Háttéradatok**. Ezt kapcsold ki, hacsak az appnak nem kell a háttérben futnia. Így egyébként akkumulátort is spórolsz.
11. **Beállítások → Alkalmazások → Különleges alkalmazás-hozzáférés**: minden pontját nézd át egyenként, és korlátozd az alkalmazások hozzáférését. Például **Hozzáférés minden fájlhoz**: ne engedd az alkalmazásoknak. **Ismeretlen alkalmazások telepítése**: ezt se engedd, így ha bármit le akarsz tölteni, külön

rákérdez majd még egyszer a telefon. **Wi-Fi vezérlés**: ha bekapcsolva van, akkor az adott alkalmazás ki-be tudja kapcsolni a Wi-Fi-t. Jobb fent a három pöttyre koppintva, **Rendszer megjelenítése**: a rendszer-alkalmazások is megjelennek, ezeknél is be lehet állítani a korlátozásokat.

12. **Beállítások → Értesítések → Bővített értesítések is kikapcsolva:** ezzel a cél az, hogy ne érkezzenek javaslatok különböző műveletekre, válaszokra. A bővített értesítések ugyanis - ahogy azt a felugró figyelmeztetés is írja – hozzáférhet személyes adatokhoz, névjegyekhez, üzenetekhez is. Tartsuk tehát kikapcsolva.
13. **Beállítások → Megjelenítés → Lezárási képernyő:** alapvetően az a cél, hogy a lezárt képernyőn minél kevesebb információ jelenjen meg. **Értesítések a lezárási képernyőn → Kompakt nézet:** az a legjobb, ha mindhárom lehetőség kikapcsolva, esetleg a **Megtekintett értesítési ikonok megjelenítése** lehet bekapcsolva, ez azt jelenti, hogy az értesítést küldő alkalmazás ikonja lesz látható a lezárt képernyőn, de az értesítés tartalma nem. Ha átváltunk **Teljes listára,** itt van lehetőség a **Megtekintett értesítések megjelenítésére,** ha ezt kipipálva hagyod, a zárolt képernyőn az értesítések tartalma is megjelenik majd. Ha például üzeneted érkezik, nemcsak annyit fogsz látni, hogy üzeneted jött, hanem annak teljes tartalmát is, ami biztonsági szempontból nem egy jó opció.
    Egyet visszalépünk, **Szöveg a lezárási képernyőn** nincs! **Eszközvezérlők használata** kikapcsolva: ez is egy támadási felület lehet. Ha olyan külső eszközt csatlakoztatsz a telefonhoz, amelynek gyakorlatilag admin joga van, akkor képes lesz a telefon vezérlésére. Ha ezt a lehetőséget kikapcsolod, akkor lezárt telefonnál ez a lehetőség nem működik. **Koppintás a telefon megtekintéséhez** kikapcsolva. **Ellenőrzés felemeléssel** kikapcsolva. **Képernyő ébresztése értesítéskor** kikapcsolva, így a lezárt képernyő nem jelez semmilyen értesítéskor, csak a feloldás után látod az értesítést. Visszalépünk egyet, **Képernyő időkorlátja:** minél rövidebb, annál jobb**,** 1-2 perc az ideális, ezután magától lezár a telefon.

Ezekkel a beállításokkal egy-egy lépést teszel afelé, hogy a telefonodon lévő adatok, információk minél nagyobb biztonságban legyenek. Ez nem jelenti azt, hogy ha akár egyet is nem fogadsz meg, akkor felesleges a Mosaic OS használata. Ezt az operációs rendszert úgy fejlesztettük, hogy az alapbeállításokkal használva is sokkal biztonságosabb körülményeket teremt a rólad szóló információknak, mint a ma használt, legelterjedtebb operációs rendszerek.