

KIBERBIZTONSÁG ÉS ONLINE BIZTONSÁG



Az eszköz fizikai védelme

- Frissítsd az operációs rendszert a lehető leggyakrabban!
- Használj tűzfalat és vírusirtó szoftvert!
- Alkalmazz biztonságos azonosító mintát, például ujjlenyomatot, különösen akkor, ha másokkal is megosztod a készüléket.

Biztonságos böngészés

- Használd a legelterjedtebb és közkedvelt böngészőket.
- Ne telepíts alkalmazásokat olyan helyekről, amelyek nem hivatalosak! Csak megbízható áruházakat vagy fejlesztői weboldalakat és megbízható webhelyeket használj.
- Ne feledd, hogy a megbízható webhelyek neve https-szel kezdődik...

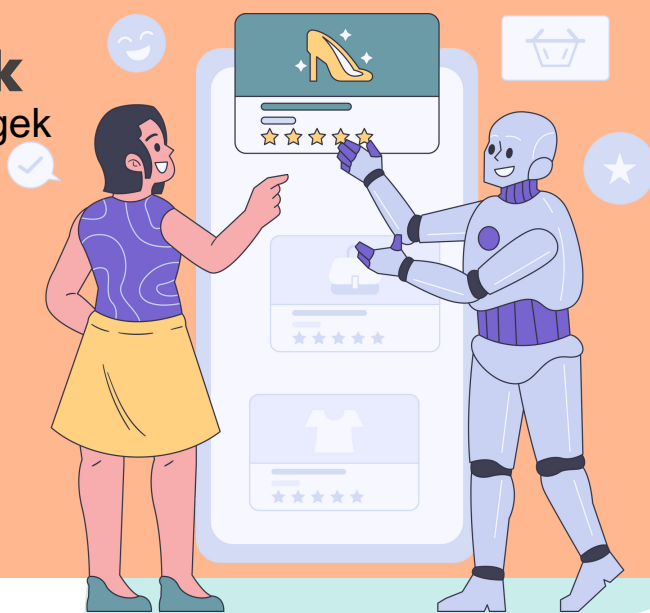


Biztonságos online kapcsolat

Az interneten való tartózkodás során a biztonságos kapcsolat létfontosságú. Ne használj nyílt wifit, ha olyan alkalmazásokba és weboldalakra lépsz be, ahol személyes adatokat kell megadni a belépéshez. Minden alkalomra használj erős jelszavakat, amelyeket nem lehet könnyen kitalálni.

Online fenyegetések – Rosszindulatú programok

Ezek a közismert nevükön vírusok és férgek olyan rosszindulatú szoftverek, amelyek rongálják a gépet vagy a rendszert. A kéretlen e-mailek (spamek) vagy felugró ablakok megpróbálják begyűjteni az adataidat vagy megtévesztenek. Ezek elkerülése érdekében ne nyisd meg az ismeretlen feladóktól érkező üzeneteket.



További ingo

digi-aware-elearninghub.com