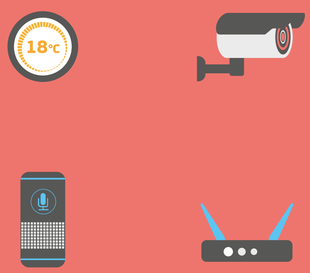
Tippek az otthoni kiberbiztonság megteremtéséhez

A dolgok internete (IoT) az internethez csatlakoztatható valamennyi eszköz hálózata. Elképzelhető, hogy Ön egyből a laptopjára vagy intelligens televíziójára gondol, azonban a dolgok internete olyan dolgokat is magában foglal, mint a játékkonzolok, a lakásvezérlő rendszerrel együttműködő készülékek, a lakásriasztó vagy a babaőr.

Miközben ezek az eszközök javíthatják életünket és munkavégzésünket, ne feledkezzünk meg arról, hogy minden, ami az internethez kapcsolódik, ki van téve a hackerek támadásainak. Íme néhány lépés az otthona védelme érdekében.



1. Tegye biztonságossá az összes eszközét!

Gondoskodjon arról, hogy valamennyi eszközét erős jelszavakkal védje, vagy állítson be kétfényezős hitelesítést (2FA), amely a dolgok internetének legtöbb eszközén elérhető!

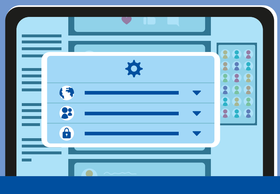
Változtassa meg az alapértelmezett jelszót és a hálózat nevét is! Nem szabad megfeledkeznie arról, hogy hálózatának neve ne tartalmazzon olyan információt, amely tájékoztatást ad otthonáról vagy családjáról, például az Ön nevéről vagy címéről.

2. Ellenőrizze alkalmazásait!

Az alkalmazások a hivatalos alkalmazás-áruházakból (Google Play, Apple App Store stb.) tölthetők le a legbiztonságosabban. Ha egy alkalmazást tetszőleges linkre kattintva tölt le, az az eszköze megfertőződéséhez vezethet.

A telepítés előtt gondosan mérlegelje, milyen információkat ad meg és milyen engedélyeket hagy jóvá! Rendszeresen vizsgálja felül alkalmazásait, és távolítsa el a szükségteleneket.

3. Tekintse át a közösségimédia-fiókjainak adatvédelmi beállításait!



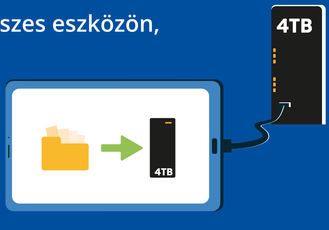
Navigáljon a felhasználói fiókja adatvédelmi beállításaihoz, ahol kiválaszthatja azokat a beállításokat, amelyek a legjobban megfelelnek Önnek!

Alaposan gondolja át, hogy milyen információkat kell feltüntetni a profiljában, a platformok kérhetnek olyan információkat, amelyeket nem kell megadnia.

4. Állítson be automatikus frissítéseket az összes eszközön, és készítsen biztonsági másolatot adatairól!

Az IoT-eszközök ki vannak téve a hackerek támadásainak, ezért a legújabb frissítések elengedhetetlenek ahhoz, hogy az Ön eszközei biztonságban legyenek. Az automatikus frissítések beállítása azt jelenti, hogy nem kell észben tartania, hogy személyesen végrehajtsa azokat.

Gondoskodjon arról, hogy legyen másolata arról, ami fontos az Önnek - például a fényképeiről vagy a kontaktokról - amit tároljon valahol offline vagy a felhőben!



5. Különítse el a munkához használt és az otthoni eszközeit!

Javasoljuk, hogy külön eszközöket használjon munkára és otthoni tevékenységeihez! A munkához használt eszközét csak munkavégzésre tartsa fenn, ami segít Önnek abban, hogy minimalizálja a veszteségeket, ha eszközét támadás éri.

Ha egy eszközt meg kell osztania, gondoskodjon arról, hogy minden felhasználó külön felhasználói profillal rendelkezzen!

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth

#ThinkB4UClick