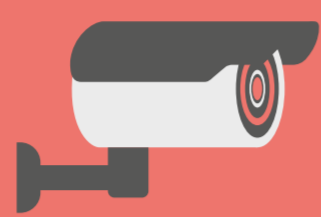


Najlepšie tipy, ako si zabezpečíte svoj domov z pohľadu kybernetickej bezpečnosti

Internet vecí (IoT) je sieť všetkých zariadení, ktoré možno pripojiť na internet. Možno vám hneď zide na um váš notebook alebo smart televízor, ale IoT zahŕňa aj veci, ako sú herné konzoly, domáci asistenti, vaše domové zabezpečovacie zariadenie alebo detské monitorovacie zariadenie.

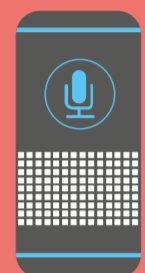
Hoci tieto zariadenia dokážu zlepšiť náš život alebo prácu, pamätajte na to, že čokoľvek, čo je pripojené na internet, môžu napadnúť hackeri. Ponúkame niekoľko tipov, ako si môžete ochrániť svoj domov.



1. Zabezpečte všetky zariadenia

Uistite sa, že všetky vaše zariadenia sú chránené silnými heslami, alebo si zriadte viacstupňové overenie, ktoré umožňuje väčšina zariadení IoT.

Mali by ste si zmeniť aj výrobcom prednastavené heslo a názov siete. Je dôležité pamätať na to, aby názov siete neobsahoval žiadne údaje, ktoré by mohli útočníkovi poskytnúť informácie o vašom domove alebo rodine, napríklad vaše meno alebo adresu.

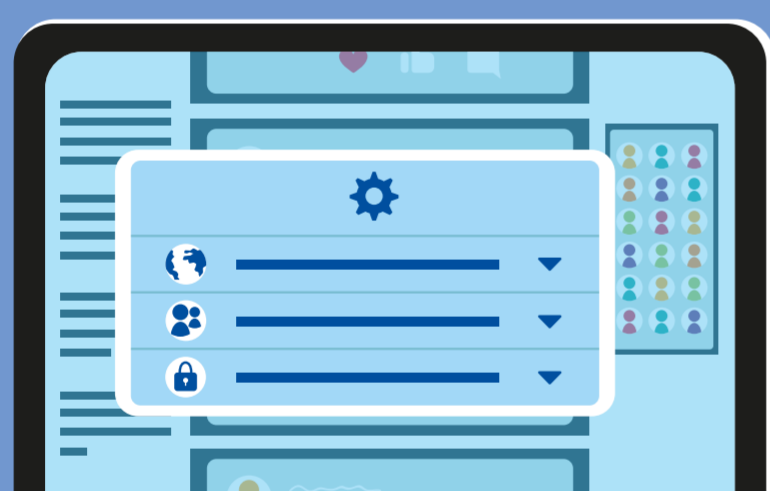


2. Skontrolujte si aplikácie

Najbezpečnejší spôsob, ako získať aplikácie, je stiahnuť ich priamo z oficiálneho obchodu s aplikáciami (Google Play, Apple App Store atď.). Kliknutím na náhodný odkaz na stiahnutie aplikácie by ste si mohli infikovať vaše zariadenie.

Pred inštaláciou dôkladne zvážte, aké údaje a súhlasy poskytujete.

Pravidelne kontrolujte svoje aplikácie a tie nepotrebné odstráňte.



3. Skontrolujte si nastavenia súkromia na vašich účtoch na sociálnych sieťach

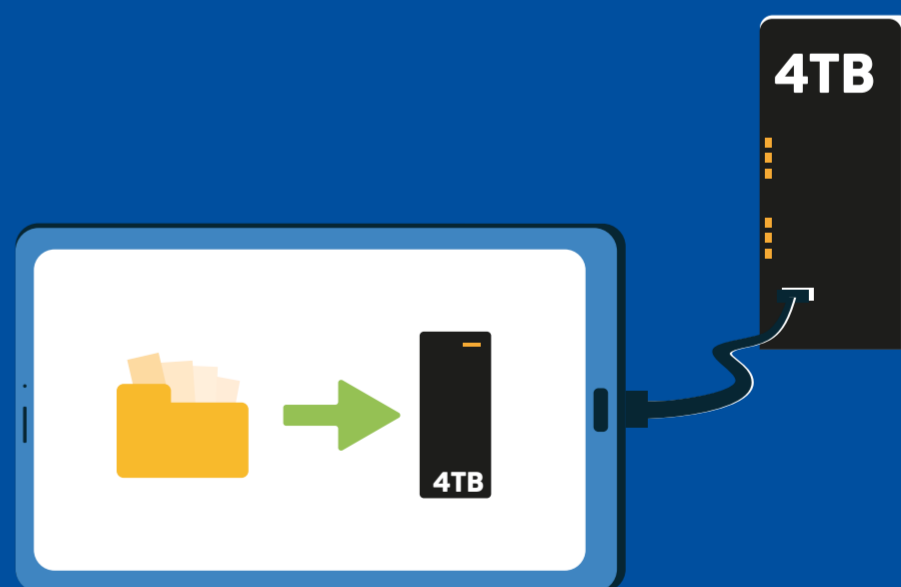
Chodte do nastavení súkromia vášho účtu, a zvoľte také nastavenia, ktoré vám budú vyhovovať.

Dôkladne zvážte, aké osobné údaje uvediete na svojom profile. Platformy mnohokrát požadujú informácie, ktoré im nie ste povinní poskytnúť.

4. Nastavte si automatické aktualizácie na všetkých zariadeniach a zálohujte si údaje

Zariadenia IoT sú zraniteľné voči útokom hackerov, preto najnovšie aktualizácie sú kľúčovou časťou ochrany vašich zariadení. Nastavenie automatických aktualizácií znamená, že si ich nebudete musieť pamätať a robiť ich sami.

Uistite sa, že máte niekde fyzicky alebo na cloude uložené kópie toho, čo je pre vás dôležité, napríklad fotky alebo kontakty.



5. Pracovné a domáce zariadenia majte oddelené

Navrhujeme, aby ste používali odlišné zariadenia pre pracovné a pre domáce účely. Zariadenia, ktoré používate na prácu, by mali byť určené len na pracovné účely. Pomôže vám to minimalizovať straty v prípade prelomenia ochrany vášho zariadenia.

Ak jedno zariadenie používate viacerí, každý používateľ nech používa samostatný používateľský profil.

