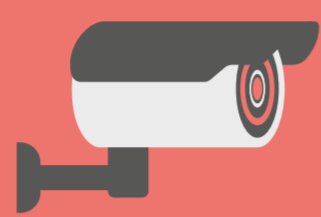


Ključni nasveti za kibernetsko varen dom

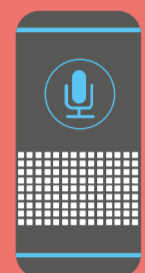
Internet stvari je omrežje vseh naprav, ki jih je mogoče povezati z internetom. Morda takoj pomislite na svoj prenosni računalnik ali pametno televizijo, a internet stvari vključuje tudi stvari, kot so igralne konzole, naprave za domača opravila, vaš hišni alarm ali elektronska varuška.

Čeprav nam lahko te naprave izboljšajo življenje in delo, lahko vse, kar je povezano z internetom, ogrozijo napadi hekerjev. Pri zaščiti svojega doma pred napadalci si lahko pomagate s sledečimi ukrepi.



1. Zaščitite vse svoje naprave

Poskrbite, da so vse vaše naprave zaščitene z močnimi gesli. Vključite tudi dvofaktorsko avtentikacijo (2FA), ki je na voljo na večini naprav interneta stvari.



Spremeniti morate tudi privzeto geslo in ime omrežja. Pomembno je, da v ime svojega omrežja ne vključite ničesar, kar bi sporočalo kar koli o vašem domu ali družini, na primer svoje ime ali naslov.

2. Preverite svoje aplikacije

Najvarneje je, da si aplikacije prenašate neposredno iz uradnih trgovin z aplikacijami (Google Play, Apple App Store itd.). S klikom na naključno povezavo za prenos aplikacije se lahko vaša naprava okuži.

Pred namestitvijo skrbno preverite, katere informacije in dovoljenja s tem posredujete.

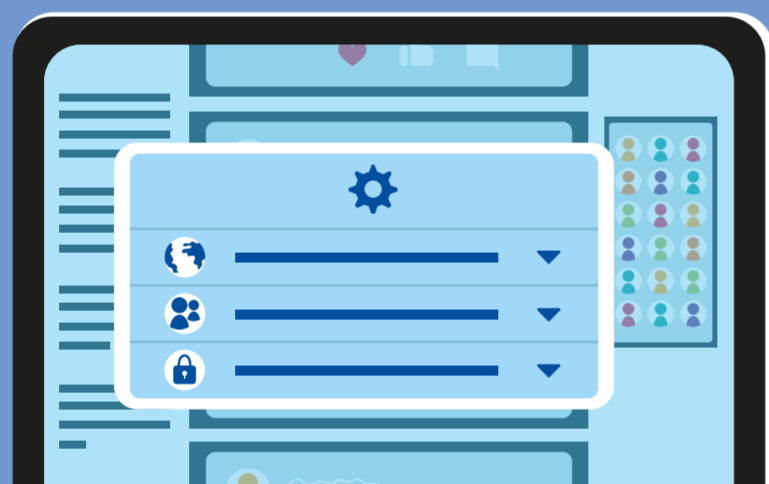
Aplikacije redno pregledujte in odstranite nepotrebne.



3. Preverite nastavitve zasebnosti v svojih računih na družbenih omrežjih

Pojdite na nastavitve zasebnosti svojega računa in izberite urezne.

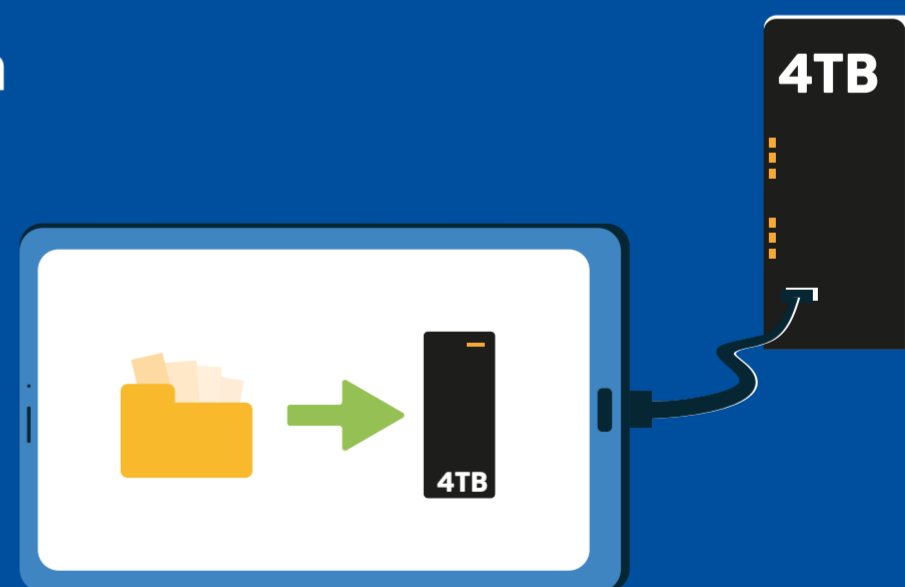
Skrbno razmislite o informacijah, ki jih navedete v profilu. Platforme vas lahko zaprosijo za informacije, ni pa vam jih treba posredovati.



4. Nastavite samodejne posodobitve na vseh napravah in podatke varnostno kopirajte

Naprave interneta stvari so izpostavljene napadom hekerjev, zato najnovejša posodobitev bistveno prispeva k ohranjanju varnosti vaših naprav. Nastanitev samodejnih posodobitev pomeni, da zanje ne bo treba skrbeti vam.

Poskrbite, da imate kopije pomembnih datotek in dokumentov (npr. fotografije, kontakte) shranjene na zunanjem disku ali v oblaku.



5. Ločujte svoje delovne in domače naprave

Svetujemo vam, da uporabljate ločene naprave za službene in osebne namene.

Službeno napravo uporabljajte le za opravljanje delovnih nalog, saj bo v primeru krave naprave izguba manjša.

Če napravo uporablja več uporabnikov, preverite, ali ima vsak svoj uporabniški profil.

