Savjeti za kibernetičku sigurnost vašeg doma

Internet stvari je mreža svih uređaja koji se mogu spojiti na internet. Vjerojatno će vam prva pomisao biti laptop ili pametni televizor, ali internet stvari uključuje i igraće konzole, vašeg kućnog asistenta, protuprovalni alarm i monitor za bebe.

Svi navedeni uređaji mogu nam olakšati život i rad, ali ne smijemo zaboraviti da sve što je spojeno na internet može biti meta napada hakera. U nastavku navodimo nekoliko primjera kako se zaštititi.

Zaštitite sve svoje uređaje

Zaštitite sve svoje uređaje snažnim lozinkama ili postavite dvostruku provjeru autentičnosti, koja je dostupna na većini uređaja interneta stvari. Promijenite zadanu lozinku i naziv mreže. Važno je da naziv mreže ne sadržava ništa što bi otkrilo informacije o vašem domu ili obitelji, na primjer vaše ime ili adresu.

Provjerite svoje aplikacije

Najsigurnije je preuzeti aplikacije izravno iz službene trgovine aplikacija (Google Play, Apple App Store itd.). Ako aplikaciju pokušate preuzeti klikom na nasumičnu poveznicu, izlažete svoj uređaj opasnosti od zaraze. Prije instalacije dobro razmislite o informacijama i dozvolama koje dajete. Redovito pregledavajte aplikacije i uklonite one koje vam više nisu potrebne.

Pregledajte postavke privatnosti svojih računa na društvenim mrežama

Idite na postavke privatnosti i odaberite postavke koje vama odgovaraju. Dobro razmislite koje informacije želite uključiti u svoj profil – platforme mogu od vas tražiti informacije koje niste obvezni dati.

Odaberite postavku automatskog ažuriranja na svim uređajima i pravite sigurnosne kopije svojih podataka

Uređaji interneta stvari mogu biti meta napada hakera, pa je redovito ažuriranje ključno za sigurnost vašeg uređaja. Kada odaberete automatsko ažuriranje, više nećete morati sami brinuti o ažuriranju uređaja. Ne zaboravite napraviti kopije svega što vam je važno i pohraniti ih lokalno ili u oblaku (npr. slike ili kontakte).

Odvojite poslovno i privatno

Preporučujemo da imate zasebne uređaje za posao i za privatne potrebe. Poslovni uređaj trebalo bi koristiti isključivo u poslovne svrhe kako bi se gubici sveli na najmanju moguću mjeru u slučaju da uređaj bude ugrožen. Ako dijelite uređaj, svaki korisnik treba imati zaseban korisnički profil.

CERT.hr surfaj sigurnije

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

CARNET znanje povezuje