

Informatičku bezbednost VAŠE ORGANIZACIJE

Nalozi i dozvole

- Izbrišite nepotrebne naloge sa svojih uređaja, uključujući i naloge gostiju.
- Proverite ko ima administratorske dozvole, jer bi trebalo da ih imaju samo korisnici kojima su zaista potrebne.
- Zahtevajte od svih korisnika da koriste jake lozinke i da ih često menjaju.

Računari i mrežni uređaji

- Promenite fabričke vrednosti podrazumevanih korisničkih lozinki zaštitnih zidova (Firewalls), ličnih računara, rutera i Vaj-faj pristupnih tačaka.
- Uključite zaštitne zidove na ličnim računarima i uređajima koji povezuju vaše računare na internet.

Svi vaši uređaji

- Deaktivirajte automatsko izvršavanje (Autorun, sinhronizacija...) aplikacija i programa na vašim mobilnim uređajima i ličnim računarima.
- Uklonite aplikacije koje ne koristite sa svih svojih uređaja.

Anti-malver

- Instalirajte i aktivirajte alate za zaštitu od malvera (za imejlove i internet) na svim uređajima, uključujući mobilne telefone i tablete, i često ih skenirajte.
- Ažurirajte softver protiv malvera i zlonamernog softvera kad god postoje ažuriranja.

Softver

- Ažurirajte sav softver koji koristite čim proizvođači objave ažuriranja i popravke.
- Napravite kompletnu rezervnu kopiju, držite je na odvojenom mestu i osigurajte se da ćete znati kako da je vratite

Izvor: Španski nacionalni institut za sajber bezbednost

**Ne zaboravite da obučite i
obrazujete svoje zaposlene!**



**Safety
in Third
Sector**



Co-funded by
the European Union

Podrška Evropske komisije izradi ove publikacije ne predstavlja odobravanje sadržaja, koji odražava samo stavove autora i Komisija se ne može smatrati odgovornom za bilo kakvu upotrebu informacija sadržanih u njoj.