



KIBERNETSKA HIGIENA

Zakon o informacijski varnosti (ZInfV-1) določa, da je kibernetika dobra praksa ohranjanja varnosti in zaščite informacij v digitalnem okolju. To vključuje ukrepe in postopke, namenjene zaščiti računalniških sistemov, omrežij in podatkov pred varnostnimi grožnjami.

Bistveni in pomembni subjekti morajo v skladu z 22. členom ZInfV-1 sprejeti **tehnične, operativne in organizacijske ukrepe** za:

- zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov
- oziroma za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev
- ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve

(Varnostni ukrepi).

Varnostni ukrepi morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščita omrežnih in informacijskih sistemov in njihovega fizičnega okolja pred incidenti, ter morajo obsegati tudi osnovne prakse kibernetike higijene in usposabljanje na področju informacijske in kibernetike varnosti.

Bistveni in pomembni subjekti naj uporabljajo osnovne prakse kibernetike higijene in se usposabljaajo na področju kibernetike varnosti. Osnovne prakse kibernetike higijene lahko vključujejo:

- načela popolnega nezaupanja,
- posodobitve programske opreme,
- konfiguracijo naprav,
- segmentacijo omrežja,
- upravljanje identitete in dostopa ter ozaveščenost uporabnikov,
- organizacijo usposabljanja in ozaveščanje zaposlenih v zvezi s kibernetikimi grožnjami, lažnim predstavljanjem in tehnikami socialnega inženiringa.

Agencija Evropske unije za kibernetiko varnost (ENISA) je v ta namen objavila [osnovne dobre prakse kibernetike higijene](#) (stran je v angleščini) in priročnik [Technical implementation guidance](#) (zlasti 8. poglavje).

Tako kot skrbimo za osebno higieno, da ohranjamo svoje zdravje, s kibernetiko higieno skrbimo za 'zdravje' naših naprav in spletnih računov. Evropska agencija ENISA poudarja, da lahko vsak posameznik z nekaj preprostimi dejanji bistveno poveča svojo varnost – ne glede na tehnično znanje.

Osnovne dobre prakse kibernetike higijene

1. Uporabljajte močna gesla

- Ustvarite močna in edinstvena gesla, ki jih je težko uganiti (kombinacija črk, števil in posebnih znakov).
- Ne uporabljajte istega gesla za več računov.
- Uporabljajte upravljalnik gesel za varno shranjevanje in ustvarjanje gesel.
- Preverite, ali so vaši računi vključeni v znane vdore podatkov, in zamenjajte gesla za prizadete storitve.

2. Omogočite večfaktorsko avtentikacijo (MFA)

- Dodajte dodatno plast zaščite tako, da omogočite MFA na svojih računih.
- Uporabljajte avtentikacijske aplikacije ali SMS-kode za preverjanje identitete.

3. Redno posodablajte programsko opremo

- Posodablajte operacijski sistem, aplikacije in protivirusno programsko opremo.
- Kjer je mogoče, omogočite samodejne posodobitve, da imate vedno najnovejše varnostne popravke.

4. Previdnost pri e-pošti, povezavah in brskanju po spletu

- Ne klikajte povezav ali prenosov iz neznanih ali sumljivih e-sporočil.
- Vedno preverite identiteto pošiljatelja, preden posredujete občutljive podatke.
- Premislite, ali je prošnja za vaše osebne podatke primerna.

5. Varnostno kopirajte pomembne podatke

- Redno ustvarjajte varnostne kopije pomembnih datotek na zunanji disk ali v oblak.
- Poskrbite, da so varnostne kopije varno shranjene in preizkušene za obnovitev podatkov.

6. Zavarujte svojo Wi-Fi omrežje

- Uporabljajte močno šifriranje (WPA3) za svoje omrežje.
- Zamenjajte privzeto geslo usmerjevalnika in uporabite močno geslo.
- Onemogočite oddaljeno upravljanje in nepotrebne storitve na usmerjevalniku.
- Varne prakse na daljavo.

7. Uporabljajte protivirusno in protizlonamerno programsko opremo

- Namestite zanesljivo protivirusno in protizlonamerno programsko opremo.
- Redno izvajajte preglede, da zaznate in odstranite grožnje.

8. Izobražujte sebe in druge

- Bodite na tekočem z najnovejšimi kibernetскими grožnjami in trendi.
- Udeležujte se izobraževanj in programov ozaveščanja o kibernetiski varnosti.
- Delite znanje z družino, prijatelji in sodelavci ter spodbujajte dobro kibernetisko higieno.

9. Omejite deljenje osebnih informacij

- Premislite, katere osebne informacije delite na spletu.
- Preverite nastavitve zasebnosti na družbenih omrežjih in drugih spletnih storitvah.

10. Spremljajte svoje račune in naprave

- Redno preverjajte finančne račune in spletne profile za sumljive dejavnosti.
- Uporabljajte varnostno programsko opremo za zaznavanje nepooblaščenega dostopa ali nenavadnega vedenja naprav.

Povezave - ostanite obveščeni

- Točka osveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje [Safe.si](https://www.safe.si).
- Program [Varni na internetu](https://www.varni-na-internetu.si).
- Brezplačni spletni tečaj iz informacijske varnosti za zaposlene [Varni v pisarni](https://www.varni-v-pisarni.si).
- Projekt ozaveščanja spletne varnosti članic Združenja bank Slovenije, bank in hranilnic, [Pazi.se](https://www.pazi.se).
- Svetovalna linija za težave na spletu [Tom telefon](https://www.tomtelefon.si) 116 111.
- Anonimna spletna prijava posnetkov spolnih zlorab otrok [Spletno oko](https://www.spletno-oko.si).
- Spletna stran [European Cybersecurity Month \(ECSM\)](https://www.ecsm.eu), kjer boste našli uporabne materiale, praktične nasvete in priporočila za varno spletno vedenje.
- Preizkusite svoje znanje o kibernetiski varnosti v [ECSM kvizu](https://www.ecsm.eu/kvizu).
- Igra [Treasure Hunt](https://www.treasure-hunt.eu) (v angleščini) za osnovne šole – prejemnico 1. nagrade ECSM za najboljši izobraževalni material 2022 (Grčija).
- [Pravljice o varni uporabi interneta](https://www.pravljice-o-varni-uporabi-interneta.si) (v angleščini), Zmagovalec 1. nagrade ECSM za najboljši video leta 2024 iz Belgije.