

Kibernetska kriminaliteta v slovenskem lokalnem okolju

ERVIN STOJNŠEK mag. ekonomskih in poslovnih ved
UNIVERZA V MARIBORU | UNIVERSITY OF MARIBOR
FAKULTETA ZA VARNOSTNE VEDE | FACULTY OF CRIMINAL JUSTICE AND SECURITY
ŽELEZNA CESTA 18, 1000 LJUBLJANA, SLOVENIJA
ERVIN.STOJNSEK@POLICIJA.COM

SLOVENJ GRADEC, 29. 9. 2026

Dejstva

- Digitalizacija družbe se je vzpostavila v zadnjih dveh desetletjih.
- Digitalni trend v povprečju prehiteva vsaj 1,5 generacijo slovenske populacije, ki v realnem svetu ne prepozna kibernetских tveganj.
- Mikro, mala in srednja podjetja predstavljajo hrbtenico slovenskega gospodarstva. Ta podjetja pogosto nimajo ustreznih varnostnih sistemov, ne izvajajo rednih varnostnih pregledov ali nimajo zaposlenega specializiranega kadra.

Dejstva

- Razvoj digitalizacije spremlja kibernetika kriminaliteta kot njen negativni učinek, z vplivi s katerimi se spopada tudi slovensko lokalno okolje.
- Digitalizacija družbe in družbenih procesov izrazito povečuje možnosti, da žrtev spletnega kriminala postane vsakdo, neglede na njegovo družbeno vlogo, lokacijo na zemljevidu ali vrsto dejavnosti, s katero se ukvarja.
- Obraz kibernetike kriminalitete v lokalnem okolju se najpogosteje izrisuje skozi kazniva dejanja spletnih goljufij, vdorov v informacijske sisteme ter krajo osebnih podatkov z vsem kar temu sledi.

Dejavniki tveganja

- **Dejavniki tveganja, ki izhajajo iz nas;**

Starost, spol, izobrazba, socialnoekonomski status, poklic in geografska lokacija, ki v medsebojni interakciji vplivajo na stopnjo ranljivosti posameznika.

- **Dejavniki tveganja, ki izhajajo iz spletnega okolja;**

Različne vrste in oblike napadov, in sicer; zaklepanje podatkov na daljavo oz. t.i ransomware napadi, zloraba zaupanja žrtve in posledično oškodovanje (goljufija), ribarjenje oz. phishing napadi, kraja, zloraba osebnih podatkov...

Analiza spletne kriminalitete v Sloveniji

V letu 2025 je bilo v Republiki Sloveniji obravnavanih in s kazensko ovadbo policije zaključenih 2.549 spletnih kaznivih dejanj.

V primerjavi z letom 2024, ko je bilo zaključenih 1.834 kaznivih dejanj, gre za 18 % porast kaznivih dejanj.

Nastala premoženjska škoda v letu 2024 je znašala 32.158.700 EUR, v letu 2025 pa 40.621.000 EUR.

Oblike kibernetске kriminalitete in nastala premoženjska škoda v letu 2025

	Število kaznivih dejanj	Škoda v EUR
investicijska vlaganja	1.037	25.420.000
BEC/CEO (direktorske prevare)	68	5.733.000
e-banke	122	5.043.000
romantična prevara	56	1.639.000
nikoli dostavljen artikel	646	1.600.000
nigerijska prevara	17	160.000
sklenitev pogodbe	121	383.000
sorodnik v težavah	10	22.000
pridobitev kredita	41	176.000
zloraba plačilne kartice	431	445.000

Primerjava različnih oblik kibernetске kriminalitete v letih 2024 in 2025

	Število kaznivih dejanj (2024)	Število kaznivih dejanj (2025)	Porast/upad (%)
investicijska vlaganja	705	1.037	+47,09
BEC/CEO (direktorske prevare)	64	68	+6,25
e-banke	90	122	+35,56
romantična prevara	46	56	+21,74
nikoli dostavljen artikel	886	646	-27,09
nigerijska prevara	16	17	+6,25
Microsoft	16	1	-93,75
sklenitev pogodbe	58	121	+108,62
sorodnik v težavah	0	10	/
pridobitev kredita	28	41	+46,43
zloraba plačilne kartice	88	431	+389,77
igre na srečo	4	0	-100,00

Primerjava materialne škode različnih oblik kibernetske kriminalitete v letih 2024 in 2025

	Škoda v EUR (2024)	Škoda v EUR (2025)	Porast/upad (%)
investicijska vlaganja	19.516.000	25.420.000	+30,25
BEC/CEO (direktorske prevare)	2.270.000	5.733.000	+152,56
e-banke	2.742.000	5.043.000	+83,92
romantična prevara	574.000	1.639.000	+185,54
nikoli dostavljen artikel	4.669.000	1.590.000	-65,75
nigerijska prevara	260.000	160.000	-38,46
Microsoft	150.000	640	-99,57
sklenitev pogodbe	314.000	383.000	+21,97
sorodnik v težavah	0	22.000	/
pridobitev kredita	98.000	176.000	+79,59
zloraba plačilne kartice	243.000	445.000	+83,13
igre na srečo	7.500	0	-100,00

Zaključek

Za učinkovito obvladovanje navedenih izzivov so nujne večplastne spremembe, ki vključujejo:

- izobraževanje in sistematično ozaveščanje prebivalstva,
- krepitev institucionalne zmogljivosti z večjim številom strokovnjakov ter napredno tehnično opremljenostjo,
- krepitev sodelovanja med javnim in zasebnim sektorjem (izmenjava informacij in skupno delovanje),
- preventivni ukrepi (uvedba varnostnih standardov, redne varnostne revizije in izvajanje simulacij napadov, za večjo odpornost sistemov),
- Celovito obravnavanje sodobne kriminalitete, ki zahteva usklajeno delovanje zakonodaje, tehnologije, strokovnega kadra in družbe kot celote.