

KIBERNETSKA KRIMINALITETA V SLOVENSKEM LOKALNEM OKOLJU

ERVIN STOJNŠEK

Policijska uprava Celje, Sektor kriminalistične policije, Celje, Slovenija
ervin.stojnsek@policija.si

Razvoj digitalizacije spremlja kibernetska kriminaliteta kot njen negativni učinek, z vplivi katere se spopada tudi slovensko lokalno okolje. Obraz kibernetske 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. Posebej ranljive za tovrstno obliko kriminalitete so manjše občine, lokalna podjetja, obrtniki in posamezniki, ki pri svojem delu ne razpolagajo z zadostno ravno ustreznega znanja o varni uporabi interneta in kibernetske zaščite. Obravnavan prispevek analizira ključne (izvršitvene) oblike tovrstnih kaznivih dejanj in dejavnike tveganja, s katerimi se srečuje policija pri njenem preiskovanju na lokalnem nivoju. Ob tem poseben poudarek namenjamo vplivu digitalizacije, povprečno nizki ravni kibernetske pismenosti ter globalni naravi kibernetske kriminalitete, ki posega v vse nivoje kibernetskega sveta.

DOI

[https://doi.org/
10.18690/um.fvv.4.2026.9](https://doi.org/10.18690/um.fvv.4.2026.9)

ISBN

978-961-299-170-8

Ključne besede:

kibernetska kriminaliteta,
lokalni nivo,
informacijska varnost,
digitalizacija,
socialni inženiring



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fvv.4.2026.9](https://doi.org/10.18690/um.fvv.4.2026.9)

ISBN
978-961-299-170-8

Keywords:
cybercrime,
local level,
information security,
digitalization,
social engineering

CYBERCRIME IN THE SLOVENIAN LOCAL ENVIRONMENT

ERVIN STOJNŠEK

Police Directorate Celje, Sector of Criminal Police, Celje, Slovenia
ervin.stojnsek@policija.si

The development of digitalization is accompanied by cybercrime as a negative effect, which is also being experienced in the Slovenian local environment. The face of cybercrime in the local environment is most often depicted by criminal offences such as online fraud, hacking into information systems, and theft of personal data, with everything that follows. Particularly vulnerable to this form of crime are smaller municipalities, local companies, craftsmen, and individuals who do not have a sufficient level of appropriate knowledge about the safe use of the Internet and cyber protection in their work. The article analyses the key (executive) forms of such crimes and the risk factors that the police encounter when investigating them at the local level. In doing so, we place special emphasis on the impact of digitalization, the average low level of cyber literacy, and the global nature of cybercrime, which affects all levels of the cyber world.



University of Maribor Press

1 Uvod

Digitalizacija družbe, razširjena uporaba elektronskih komunikacijskih sredstev ter globalna dostopnost spletnih storitev pomembno in nepovratno prispevajo k povečanju števila kaznivih dejanj, storjenih z uporabo informacijskih sistemov ali usmerjenih zoper njih. Pri tem ne gre več zgolj za posamične, oportunistične storilce, temveč za dobro organizirane kriminalne združbe, ki delujejo globalno, z uporabo naprednih tehnik prikrivanja sledi ter izkoriščanjem razdrobljenosti posameznih jurisdikcij.

Policija vsako leto zaznava porast števila prijav posameznih kaznivih dejanj, čemur sledi naraščanje finančne škode zaradi teh kaznivih dejanj. Spletna kriminaliteta, ki temelji na socialnem inženiringu in zlonamerni uporabi različne programske opreme, zahteva od policistov in kriminalistov visoko stopnjo specializiranih znanj, stalno tehnično nadgrajevanje orodij za delo in učinkovito operativno koordinacijo.

Policija v Republiki Sloveniji tovrstne preiskave v veliki meri obravnava razdrobljeno po različnih organizacijskih enotah, praviloma glede na kraj bivališča oškodovanca. Tako je v letu 2025 tovrstne zadeve obravnavalo 7 različnih enot na ravni sektorjev kriminalistične policije (SKP) ter 75 različnih policijskih postaj. Največje slabosti tovrstnega načina dela so, da je celostni pregled nad (povezanimi) primeri in obravnavo kriminalnih združb otežen in da se opravila v posameznih preiskovalnih postopkih podvajajo (Ministrstvo za notranje zadeve, Policija, 2026).

Tako se v policiji povečuje potreba po strateškem načrtovanju, analitični podpori, sistematičnem razvoju preiskovalnih metod ter okrepljenem sodelovanju z domačimi in tujimi institucijami. V takšnih razmerah postaja nujna vzpostavitev organizacijske strukture, ki bo omogočala celostni, usklajen in dolgoročno vzdržen pristop k obravnavi kibernetške kriminalitete.

2 Opredelitev in značilnosti kibernetške kriminalitete

Kibernetška kriminaliteta obsega kazniva dejanja, ki se opravljajo z uporabo informacijskih in komunikacijskih tehnologij ali so usmerjena proti njim. V širšem smislu zajema dejanja, pri katerih so računalniški sistemi in omrežja sredstvo izvršitve (npr. spletne goljufije), kot tudi dejanja, pri katerih so ti sistemi neposredna tarča napada (npr. nepooblaščen dostop, napadi na informacijske sisteme). Gre za

dinamično obliko kriminalitete, ki se razvija vzporedno s tehnološkim napredkom. Kibernetška kriminaliteta se odlikuje tudi po visoki stopnji prilagodljivosti, saj storilci hitro izkoriščajo nove tehnologije in ranljivosti sistemov. Poleg tega ima pomembno lastnost nizkih vstopnih ovir, saj so na voljo številna orodja in storitve (npr. *crime-as-a-service*), ki omogočajo izvrševanje kaznivih dejanj tudi manj tehnično usposobljenim posameznikom (Ministrstvo za notranje zadeve, Policija, 2026). Za kibernetško kriminaliteto je značilna tudi težavna dokazljivost, saj so digitalni dokazi pogosto razpršeni, lahko spremenljivi in zahtevajo ustrezno forenzično obravnavo. Posledično sta odkrivanje in pregon teh dejanj kompleksna ter zahtevata mednarodno sodelovanje in interdisciplinarni pristop.

3 Specifika lokalne ravni v Sloveniji

Slovenija v družbenem smislu sledi trendom digitalizacije, kar vključuje elektronsko poslovanje, e-upravo, digitalne finančne storitve itd. Digitalizacija družbe se je tako vzpostavila v zadnjih dveh desetletjih. Digitalni trend v povprečju prehiteva vsaj 1,5 generacije slovenske populacije, ki v realnem svetu ne prepozna kibernetških tveganj, ki izhajajo iz t. i. *phishing* napadov, socialnega inženiringa, neustrezne uporabe zaščitnih gesel ter nepazljivost pri ravnanju z osebnimi podatki.

3.1 Ranljivost malih in srednjih podjetij

Mala in srednja podjetja predstavljajo hrbtenico slovenskega gospodarstva, vendar pogosto nimajo ustreznih varnostnih sistemov, ne izvajajo rednih varnostnih pregledov ali nimajo zaposlenega specializiranega kadra. Posledično so pogosta tarča kibernetških napadov, ki so v praksi videti kot (Ministrstvo za notranje zadeve, Policija, 2026):

1. *ransomware* napadi, kjer žrtev nezavedajoč se nevarnosti na svojo elektronsko napravo omogoči namestitev zlonamerne programske opreme (angl. *malware*), ki napadalcu omogoči vzpostavitev nadzora nad napravo ter posledično žrtvi onemogoči dostop do lastnih podatkov ali sistema in nato zahteva odkupnino (angl. *ransom*) za ponovno vzpostavitev dostopa;
2. poslovne prevare oz. spletne goljufije, ki temeljijo izključno na zlorabi zaupanja, ki ga storilci ustvarijo pri žrtvi z uporabo metod socialnega inženiringa;
3. *phishing* napadi, ki se opravljajo s sočasnim pošiljanjem mase lažnih e-sporočil, lažnih oglasnih sporočil in

4. kraje podatkov, ki se izkazujejo kot zloraba osebnih podatkov, sklepanje lažnih poslov ali finančne prevare.

4 Dejavniki tveganja

Med ključne dejavnike tveganja sodijo starost, spol, izobrazba, socioekonomski status, poklic in geografska lokacija, ki v medsebojni interakciji vplivajo na stopnjo ranljivosti posameznika. Starost je eden najpomembnejših dejavnikov: mlajši posamezniki so zaradi pogoste uporabe digitalnih tehnologij bolj izpostavljeni napadom, hkrati pa se pogosteje pojavljajo kot storilci, medtem ko so starejši zaradi nižje digitalne pismenosti pogostejše žrtve kibernetške kriminalitete. Izobrazba in digitalna pismenost močno zmanjšujeta tveganje za osnovne napade, ne izključujejo pa dovzetnosti na bolj prefinjene prevare. Na vrsto napadov vpliva tudi socioekonomski status, pri čemer so posamezniki z nižjim dohodkom bolj dovzetni za preproste napade, največkrat v obliki finančnih prevar, medtem ko so premožnejši lahko tarča kompleksnejših oblik napadov. Dejavnik tveganja predstavlja tudi poklic, saj so osebe z dostopom do finančnih sredstev ali občutljivih podatkov pogostejše tarča ciljanih napadov. Ob tem je treba izpostaviti še geografsko lokacijo kot element vplivanja prek stopnje digitalizacije in učinkovitosti varnostnih mehanizmov (Ministrstvo za notranje zadeve, Policija, 2026).

5 Analiza spletne kriminalitete v Sloveniji

Podatki v analizi so zajeti iz dinamične statistike policije, pri čemer je bilo v letu 2025 v Republiki Sloveniji obravnavanih in s kazensko ovadbo 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 (Ministrstvo za notranje zadeve, Policija, 2026). Kot izhaja iz tabele 1, ugotavljamo, da je številčno največ kaznivih dejanj, ki izhajajo iz investicijskih vlaganj, sledijo nikoli dostavljeni artikli, zlorabe plačilnih kartic, vdori v e-banke, sklenitve pogodb, BEC/CEO goljufije, pridobitev kredita, romantične in nigerijske prevare, Microsoft goljufije ter igre na srečo.

Tabela 1: 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	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

Vir: Ministrstvo za notranje zadeve, Policija, 2026.

Največja škoda v povprečju na posamezno obliko kaznivih dejanj nastaja pri investicijskih vlaganjih, BEC/CEO goljufijah, vdorih v e-banke, romantičnih prevarah, vdorih v e-banke, nigerijskih prevarah. Povprečna škoda na posamezno kaznivo dejanje znaša 15.936 EUR. Modusi bodo podrobneje opisani v nadaljevanju prispevka. Kot izhaja iz tabele 2, beležimo izrazit porast prijav zlorab plačilnih kartic (389,77 %), goljufij pri sklenitvi pogodbe (108,62 %), goljufij s pridobitvijo kredita (46,43 %), investicijskih goljufij (47,09 %), vdorov v e-banke (35,56 %), romantičnih goljufij (21,74 %). Goljufije v obliki sorodnika v težavah so se pojavile prvič, v zatonu pa so goljufije z lažno tehnično pomočjo Microsoft in goljufije pri igrah na srečo.

Tabela 2: 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	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

Vir: Ministrstvo za notranje zadeve, Policija, 2026.

Izrazit porast nastale materialne škode se beleži pri romantičnih prevarah (185,56 %), BEC/CEO goljufijah (152,56 %), vdorih v e-banke (83,92 %), zlorabah plačilnih kartic (83,13 %), pridobitvah kredita (79,59 %) in investicijskih goljufijah (30,25 %). Pri drugih oblikah je beležen upad škode (tabela 3).

Tabela 3: Primerjava materialne škode različnih oblik kibernetške 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	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

Vir: Ministrstvo za notranje zadeve, Policija, 2026.

6 Sklep

Kibernetška kriminaliteta predstavlja kompleksen in večplasten izziv, ki zahteva celovit in sistemski pristop. Njena izrazita internacionalnost pomeni, da storilci pogosto delujejo iz različnih držav, kar otežuje njihovo identifikacijo, zbiranje dokaznega gradiva in učinkovito kazenskopravno obravnavo. Dodatno problematiko predstavlja nizka stopnja prijavljanja kaznivih dejanj, saj žrtve zaradi občutkov sramu, nepoznavanja postopkov ali nezaupanja v organe pregona pogosto ostajajo pasivne, kar vodi v razkorak med dejanskim in evidentiranim obsegom kriminalitete.

Pomemben omejitveni dejavnik pri obvladovanju teh pojavov predstavlja primanjkljaj strokovnjakov s področja digitalne forenzike, informacijske varnosti in analitike podatkov. Pomanjkanje ustrezno usposobljenih strokovnjakov zmanjšuje operativno učinkovitost institucij, ki se soočajo s čedalje bolj prefinjenimi oblikami kriminalnega delovanja. Hkrati hiter tehnološki razvoj omogoča nastanek novih načinov izvrševanja kaznivih dejanj, pri čemer zakonodajni okvirji in zaščitni

mehanizmi pogosto zaostajajo za dejanskimi razmerami, kar ustvarja dodatne varnostne vrzeli.

Za učinkovito obvladovanje navedenih izzivov so nujne večplastne spremembe. Ključno vlogo ima izobraževanje in sistematično ozaveščanje prebivalstva, zlasti z vidika dviga kibernetске pismenosti in razvoja programov za ranljive skupine. Prav tako je treba okrepiti institucionalne zmogljivosti z večjim številom strokovnjakov ter napredno tehnično opremljenostjo, ki omogoča učinkovito preiskovanje kompleksnih primerov. Pomemben element predstavlja tudi okrepljeno sodelovanje med javnim in zasebnim sektorjem, saj izmenjava informacij in skupno delovanje omogočata hitrejša in učinkovitejša odzivanje na varnostne grožnje. Poseben poudarek mora biti namenjen preventivnim ukrepom, kot so uvedba varnostnih standardov, redne varnostne revizije in izvajanje simulacij napadov, ki povečujejo odpornost sistemov. Celovito obravnavanje sodobne kriminalitete tako zahteva usklajeno delovanje zakonodaje, tehnologije, strokovnega kadra in družbe kot celote. Le z integriranim, proaktivnim in interdisciplinarnim pristopom je mogoče zagotoviti dolgoročno učinkovito preprečevanje in pregon kaznivih dejanj v hitro spreminjajočem se digitalnem okolju.

Učinkovito preiskovanje teh kaznivih dejanj, ki jih vse pogostejše opravljajo dobro organizirane kriminalne združbe z izrazito mednarodno razsežnostjo, zahteva ustrezno organizacijsko strukturo, specializacijo in centralizirano operativno delovanje policije. Službi generalnega direktorja policije je bil julija 2025 zato posredovan predlog za spremembo sistemizacije v okviru Uprave kriminalistične policije Generalne policijske uprave, katerega cilj je ustanovitev Sektorja za kibernetско kriminaliteto, organiziranega v treh oddelkih: Oddelek za preiskovanje kibernetске kriminalitete, Oddelek za operativno podporo ter Oddelek za strateško načrtovanje in razvoj. Predlog je zastavljen celostno in je usmerjen v sistemsko ureditev področja preiskovanja kibernetске kriminalitete. V njem so jasno opredeljene ključne problematike, povezane s preiskovanjem spletnih goljufij, spolnih zlorab otrok na spletu ter napadov na informacijske sisteme. Predvideno je, da bo sektor izvajal centralizirano preiskovanje zadev z večjim številom oškodovancev, zagotavljal učinkovitejšo koordinacijo med policijskimi enotami na vseh ravneh v državi ter omogočal okrepljeno mednarodno sodelovanje. Sektor bo vzpostavljen kot enotna centralna točka za zbiranje, obdelavo in analizo informacij s področja kibernetске kriminalitete v ožjem pomenu besede, to je kaznivih dejanj, storjenih z uporabo elektronskih komunikacijskih omrežij in informacijskih

sistemov ali usmerjenih zoper takšna omrežja in sisteme. Poleg tega bo izvajal specializirane naloge, kot so analize kriptovalut, spletno patroljiranje, dejavnosti OSINT ter spremljanje in preiskovanje vsebin na temnem spletu (angl. *dark web*).

Viri in literatura

Ministrstvo za notranje zadeve, Policija. (2026). *Letno poročilo o delu policije 2025*.
<https://www.policija.si/images/stories/Statistika/LetnaPorocila/DOC/LetnoPorocilo2025.docx>

