

**Analiza nacionalnih ukrepov
za izboljšanje varnosti elektronskih plačil in
preprečevanje goljufij pri plačilih**

KAZALO

GLOSAR.....	3
1. UVOD.....	6
2. TRENDI.....	6
3. PREPOZNAVA KLJUČNIH PODROČIJ ZA IZBOLJŠANJE VARNOSTI E-PLAČIL IN PREPREČEVANJE PLAČILNIH GOLJUFIJ.....	8
4. VARNOST E-PLAČILNIH APLIKACIJ IN PRODAJNIH MEST	8
4.2. VARNOSTNI PAKETI IN UPRAVLJANJE TVEGANJ S STRANI UPORABNIKA	10
4.3. USMERITVE ZA VARNO IN ODGOVORNO UPORABO PLAČILNIH STORITEV.....	10
4.4. ZAGOTAVLJANJE PRIČAKOVANEGA NIVOJA VARNOSTI ZA PRODAJNA MESTA.....	10
5. ODZIV, OBRAVNAVE IN IZMENJAVA PODATKOV MED DELEŽNIKI.....	11
5.1. POENOTENI TEHNIČNI UKREPI ODZIVA NA NACIONALNEM NIVOJU.....	11
5.2. NACIONALNI PROTOKOL ZA CELOVITO OBRAVNAVO PLAČILNIH GOLJUFIJ.....	12
5.3. VZPOSTAVITEV NACIONALNEGA OKVIRA ZA IZMENJAVO PODATKOV O PLAČILNIH GOLJUFIJAH	13
6. NACIONALNA PLATFORMA ZA OZAVEŠČANJE IN DIGITALNO OPISMEJENJE.....	13
7. DODATNI UKREPI NA NACIONALNEM NIVOJU	14
7.1. RAZVOJ NACIONALNIH VIROV GROŽENJ IN ORODIJ ZA DIGITALNO ODPORNOST	14
7.2. USMERITVE ZA PRIPRAVO MINIMALNIH TEHNIČNIH UKREPOV IN KONTROL ZA PRAVNE SUBJEKTE	15
7.3. OBRAVNAVA IN PODPORA PSIHOLOŠKEGA VIDIKA PLAČILNIH GOLJUFIJ	16
7.4. POENOTENJE DIGITALNE IDENTITETE IN UPORABNIŠKE IZKUŠNJE	16
8. NACIONALNA KOORDINACIJA IDENTIFICIRANIH UKREPOV	16
9. ANALIZA POTREB IN ZAHTEV ZA VZPOSTAVITEV NACIONALNEGA FORUMA	17
9.1. NALOGE, PRISTOJNOSTI IN SESTAVA FORUMA	17
9.2. IDENTIFIKACIJA DELEŽNIKOV V FORUMU IN SKUPINAH	19
10. ZAKLJUČEK	19
CITATI IN VIRI.....	20
ANEKS 1: SEZNAM IDENTIFICIRANIH DELEŽNIKOV FORUMA IN DELOVNIH SKUPIN	22

GLOSAR

- **APP goljufija (Authorised Push Payment Fraud):** Oblika plačilne goljufije, pri kateri storilec s psihološko manipulacijo prepriča uporabnika, da ta prostovoljno in zavestno sam izvede ter potrdi denarno nakazilo na račun goljufa.
- **Avtentikacija:** Postopek preverjanja identitete uporabnika ali naprave z uporabo varnostnih elementov (geslo, PIN, biometrija), ki zagotavlja, da ima dostop do plačilnih storitev upravičena oseba.
- **Blokada:** Začasna ali trajna tehnična in pravna omejitev dostopa do določenega računa ali možnosti izvajanja transakcij zaradi suma goljufije.
- **CLI (Calling Line Identification):** Tehnični podatek, ki identificira telefonsko številko kličočega. Uporablja se za preverjanje pristnosti klicev in odkrivanje lažnega predstavljanja.
- **CSIRT (Computer Security Incident Response Team):** Strokovna skupina za odzivanje na računalniške varnostne incidente, ki nudi podporo pri obravnavi in odpravi kibernetских groženj.
- **CVE (Common Vulnerabilities and Exposures):** Mednarodni sistem za standardizirano označevanje in katalogiziranje znanih računalniških ranljivosti.
- **Denarna mula:** Fizična oseba, ki zavestno ali nezavedno sodeluje pri prejemanju, prenosu ali dvigu protipravno pridobljenih sredstev za storilce goljufij, običajno v zameno za plačilo ali drugo korist.
- **Digitalna identiteta:** Skupek elektronskih podatkov, ki enolično identificirajo uporabnika v digitalnem okolju (npr. uporabniško ime, digitalni certifikat, e-osebna izkaznica).
- **Digitalna odpornost:** Zmožnost informacijskih sistemov, organizacij in uporabnikov, da se učinkovito zaščitijo, zaznajo ter odzovejo na digitalne grožnje in incidente.
- **Digitalna pismenost:** Sposobnost varne, kritične in učinkovite uporabe digitalnih tehnologij, storitev ter interneta.
- **DNS (Domain Name System):** Internetni sistem, ki pretvarja domenska imena v IP-naslove. Uporablja se tudi za filtriranje in blokiranje dostopa do zlonamernih spletnih mest na ravni omrežja.
- **Družbeni inženiring (Social Engineering):** Manipulativne tehnike, s katerimi storilci psihološko zavajajo uporabnike, da sami razkrijejo občutljive podatke ali izvedejo nezaželene finančne akcije.
- **EDR (Endpoint Detection and Response):** Varnostna rešitev za neprekinjeno zaznavanje, preiskovanje in odzivanje na napredne grožnje na končnih napravah (računalniki, mobilni telefoni).
- **EUDIW (European Digital Identity Wallet):** Evropska digitalna denarnica, ki uporabnikom omogoča varno hranjenje, uporabo in izmenjavo identifikacijskih podatkov ter drugih elektronskih dokazil v skladu z evropskim okvirom digitalne identitete.
- **FRIDA (Fraud Information Sharing Initiative):** Evropska pobuda za strukturirano izmenjavo informacij o goljufijah in povezanih tveganjih med relevantnimi deležniki z namenom hitrejšega zaznavanja in preprečevanja plačilnih goljufij.
- **Viri groženj (feed):** Avtomatizirani podatkovni viri, ki v realnem času vsebujejo informacije o aktualnih grožnjah, zlonamernih domenah, hash vrednostih in drugih indikatorjih ogroženosti.
- **Goljufija pri plačilih:** Vsako namerno zavajanje, ponarejanje ali zloraba, ki vodi do neupravičenega prenosa finančnih sredstev ali nepooblaščne pridobitve plačilnih podatkov.

- **Hash vrednost:** Kriptografski povzetek podatkov (digitalni prstni odtis), ki se uporablja za preverjanje integritete datotek ali identifikacijo zlonamerne programske opreme.
- **IOC (Indicator of Compromise):** Tehnični indikator, ki kaže na morebitno kompromitacijo sistema (npr. sumljivi IP-naslovi, zlonamerne domene, specifične hash vrednosti datotek).
- **IOF (Indicator of Fraud):** Indikator ali sumljiv vzorec obnašanja, ki kaže na morebitno izvajanje goljufije znotraj plačilnih sistemov.
- **Jailbreak/root:** Postopek odstranitve tovarniških varnostnih omejitev na operacijskem sistemu mobilne naprave, kar drastično poveča tveganje za zunanje napade.
- **Kibernetska grožnja:** Vsak potencialni dogodek ali dejanje, izhajajoče iz uporabe IKT infrastrukture, ki lahko ogrozi varnost podatkov, procesov ali sistemov.
- **Komercialni viri:** Plačljive storitve ali podatkovne baze globalnih ponudnikov, ki nudijo dodatne informacije o grožnjah, ranljivostih in zlonamernih akterjih.
- **Lažno prikazovanje identitete (Spoofing):** Tehnika, pri kateri storilec ponaredi identiteto (npr. telefonsko številko pri klicu, ime pošiljatelja SMS ali e-poštni naslov) z namenom zavajanja uporabnika.
- **MFA (Večfaktorska avtentikacija):** Varnostni mehanizem, ki od uporabnika zahteva predložitve dveh ali več neodvisnih dokazil o identiteti (npr. geslo in potrditev v mobilni aplikaciji ali biometrija) pred odobritvijo dostopa.
- **Minimalni tehnični ukrepi:** Nabor osnovnih varnostnih zahtev in tehničnih kontrol, ki zagotavljajo standardizirano raven zaščite pri ponudnikih ali uporabnikih plačilnih storitev.
- **MISP (Malware Information Sharing Platform):** Odprtokodna platforma za varno, strukturirano in avtomatizirano izmenjavo informacij o kibernetskih grožnjah med organizacijami.
- **Mobilna plačilna aplikacija:** Programska oprema na mobilni napravi, ki uporabniku omogoča varno odrejanje in izvajanje plačilnih transakcij.
- **Nacionalna platforma za ozaveščanje:** Centraliziran državni sistem za usklajeno izobraževanje, obveščanje in preventivno ozaveščanje javnosti o varnosti digitalnih storitev.
- **Nacionalni forum:** Krovno koordinacijsko in posvetovalno telo za usklajevanje ukrepov, zakonodajnih pobud ter izmenjavo informacij na področju varnosti plačil.
- **Oblachna shramba:** Spletna storitev za shranjevanje podatkov na oddaljenih strežnikih, ki omogoča varno kopiranje, arhiviranje in zaščito podatkov pred izgubo.
- **Phishing:** Vrsta spletne goljufije, pri kateri storilec prek lažnih sporočil (e-pošta, SMS) ali ponarejenih spletnih strani poskuša od uporabnika izvabiti občutljive podatke.
- **PIN (Personal Identification Number):** Osebna identifikacijska številka, ki služi kot varnostni element za potrjevanje identitete in odobritev plačilnih transakcij.
- **Plačilna shema:** Standardiziran nabor skupnih pravil, praks in standardov za izvajanje določenega plačilnega instrumenta (npr. kartične sheme Visa, Mastercard).
- **Plačilni instrument:** Vsako personalizirano orodje, naprava ali postopek, ki omogoča odrejanje plačilnih transakcij (npr. plačilna kartica, elektronska denarnica).

- **PoS-terminal:** Naprava na fizičnem prodajnem mestu, ki omogoča sprejem in obdelavo elektronskih plačil, vključno s plačili s plačilnimi karticami ter brezstičnimi plačili prek mobilnih denarnic.
- **Psihološko ujetništvo (Psychological Captivity):** Specifično stanje zmanipulirane žrtve, ki pod vplivom dolgotrajnega družbenega inženiringa in grajenja odnosa slepo zaupa storilcu, prostovoljno predaja dostope ter zavestno ignorira bančna opozorila.
- **QR-plačilne storitve:** Plačilne storitve, ki uporabniku omogočajo izvedbo plačila s skeniranjem QR-kode, ki vsebuje podatke, potrebne za samodejno pripravo in izvedbo plačilne transakcije.
- **Ranljivost:** Tehnična ali logična slabost v informacijskem sistemu, omrežju ali programski opremi, ki jo lahko napadalec izkoristi za nepooblaščen dostop.
- **Rešitve za sprejem plačil na spletnih prodajnih mestih:** Programske rešitve in storitve, ki trgovcem omogočajo sprejemanje in obdelavo elektronskih plačil na spletnih prodajnih mestih, vključno s kartičnimi plačili, digitalnimi denarnicami, takojšnjimi plačili, QR-plačilnimi storitvami in drugimi načini elektronskega plačevanja.
- **SDK (Software Development Kit):** Nabor programskih orodij, knjižnic in dokumentacije, ki razvijalcem omogoča razvoj ali vključevanje funkcionalnosti v aplikacije in informacijske sisteme.
- **Telemetrija:** Samodejno zbiranje in oddaljeno pošiljanje tehničnih podatkov o stanju ter delovanju naprave za zgodnje zaznavanje varnostnih tveganj in anomalij.
- **Threat Intelligence (obveščevalni podatki o grožnjah):** Zbiranje, analiza in izmenjava informacij o kibernetičnih grožnjah, ranljivostih, napadalcih in indikatorjih ogroženosti z namenom preprečevanja, zaznavanja in odzivanja na varnostne incidente
- **Transakcijski limit:** Najvišji dovoljeni finančni znesek za posamezno transakcijo ali skupino transakcij v določenem časovnem obdobju, ki ga lahko določi ponudnik plačilnih storitev ali uporabnik.
- **UAN (Unique Alert Number):** Edinstvena identifikacijska številka primera, ki se uporablja za usklajeno označevanje, sledenje in hitro medsebojno obravnavo goljufij med bankami ter institucijami.
- **Uporabniške omejitve storitev:** Funkcionalnost, ki uporabniku omogoča samostojno prilagajanje in zaklepanje uporabe digitalnih kanalov in plačilnih storitev, transakcijskih limitov ali geografskih območij porabe plačilnih storitev.
- **Varnostna opozorila:** Dinamična obvestila in opozorila uporabnikom o zaznanih tveganjih, sumljivih transakcijah ali potrebnih varnostnih ukrepih v realnem času.
- **Varnostni paket:** Prilagodljiv nabor varnostnih funkcionalnosti in tehničnih zaščitnih mehanizmov, ki jih ponudnik ponuja uporabniku glede na želeno raven zaščite.

1. UVOD

Digitalizacija plačilnih storitev in hitro naraščajoča uporaba spletnih ter mobilnih plačilnih kanalov pomembno spreminjata način poslovanja finančnih institucij ter vedenje uporabnikov. S tem se vzporedno povečujeta kompleksnost groženj in obseg goljufij, ki izkoriščajo šibkosti znotraj plačilnega ekosistema, zlasti pomanjkanje poenotenega in celovitega naslavljanja razvijajočih se groženj.

Neusklajenosti so zaznane tako z vidika tehničnih in varnostnih zasnov digitalnih storitev, pri možnosti poenotenja priporočenih ravnanj uporabnikov in obravnave ob goljufijah s strani ponudnikov plačilnih storitev ter v pomanjkljivih oziroma neenotnih institucionalnih okvirih za obravnavo in odziv na goljufije ter kibernetске grožnje na splošno. Ti sistemski izzivi so se v obdobju po covidu dodatno okrepili zaradi pospešene digitalizacije in množičnejšega prehoda uporabnikov na spletne in mobilne storitve, pri čemer so v digitalno okolje v večjem obsegu vstopili tudi uporabniki z nižjo stopnjo digitalne in informacijske pismenosti, katerih pričakovanja in ravnanja izhajajo iz izkušenj ter navad poslovanja v fizičnem svetu.

Prav potreba po sistemskem in usklajenem naslavljanju navedenih izzivov predstavlja izhodišče Strategija razvoja trga plačil v Sloveniji za obdobje 2024–2028, ki jo je 20. decembra 2023 sprejel Nacionalni svet za plačila (NSP). NSP vzpostavlja strateški okvir za varen, učinkovit in zaupanja vreden razvoj plačilnega ekosistema v Sloveniji ter kot enega ključnih strateških ciljev opredeljuje krepitev varnosti, odpornosti in zaupanja v elektronska plačila. Ta dokument predstavlja enega izmed izvedbenih ukrepov za uresničevanje navedenega strateškega cilja NSP in je pripravljen v okviru Delovne skupine za varnost (v nadaljevanju: DS Varnost), ki deluje kot strokovno in usklajevalno telo na tem področju (NSP, 2023).

V tem kontekstu dokument podpira strateške usmeritve NSP, pri čemer sledi cilju celovite identifikacije področij, na katerih so možne nadgradnje in poenotenje pristopov, ter pripravi predlogov ukrepov, ki bodo sledili in se prilagajali trenutnim ter prihodnjim trendom in tveganjem na področju elektronskih plačil. Dokument izhaja iz ugotovitve, da razdrobljeni in neenotni pristopi k tehnični zaščiti, obravnavi varnostnih dogodkov in ozaveščanju uporabnikov otežujejo učinkovito preprečevanje goljufij ter pravočasen in usklajen odziv nanje, zlasti v času, ko razvoj umetne inteligence omogoča storilcem hitro odkrivanje in izkoriščanje sistemskih šibkosti ter prepričljivo posnemanje pristnosti in legitimnosti komunikacije, kar dodatno zmanjšuje zmožnost prepoznavanja znakov goljufije brez visoke ravni informacijske in finančne pismenosti uporabnikov. Pri pripravi analize so bili upoštevani relevantni evropski in nacionalni viri.

2. TRENDI

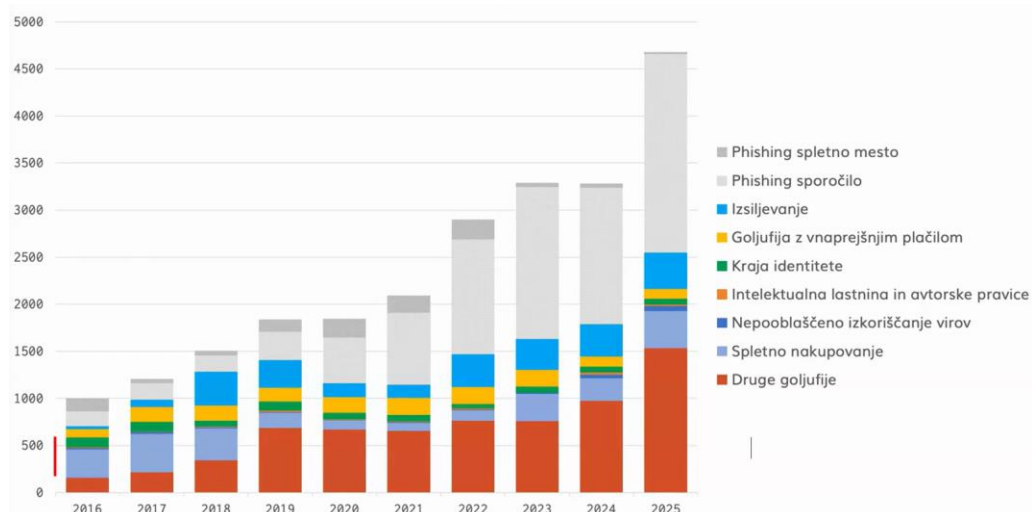
Aktualne plačilne goljufije temeljijo predvsem na socialnem inženiringu¹ ter goljufiji legitimnih komunikacijskih poti. Ta ključni premik fokusa goljufov s tehnologije na ljudi² potrjuje tudi skupno poročilo EBA in ECB o goljufijah pri plačilih iz leta 2025, ki ugotavlja, da sta se vrednost in volumen goljufij pri kreditnih plačilih, pri katerih so bile transakcije izvedene s strani plačnika kot rezultat

¹ European Payments Council (2025): "Social engineering attacks and phishing attempts are still increasing, and they remain instrumental, often in combination with malware."

² European Payments Council (2025): "Social engineering increasingly leads to authorised push payments (APP) fraud; the techniques have greatly evolved over the last years and are still evolving, as the targets are payment system users rather than technology."

manipulacije, med začetkom leta 2022 in koncem leta 2024, drastično povečala³ (EBA & ECB, 2025, str. 19-21). Storilci za izvajanje goljufij uporabljajo lažna spletna mesta, elektronsko pošto, klepetalnike, telefonske klice ter SMS sporočila⁴. Za uspešne goljufije je značilno, da se tako pisna kot govorna komunikacija izvaja v praviloma dobri in prepričljivi slovenščini, pri čemer storilci vizualno in vsebinsko posnemajo komunikacijo bank, ponudnikov storitev ali drugih zaupanja vrednih institucij.

Pogosta je tudi uporaba tehnik lažnega prikazovanja identitete, vključno s ponarejanjem slovenskih telefonskih števil, kar dodatno povečuje verodostojnost napadov. Med najpogostejše primere sodijo tudi t. i. APP goljufije (Authorised Push Payment Fraud), pri katerih uporabnik zaradi manipulacije storilca sam odredi plačilo na račun goljufa. Takšne goljufije praviloma ne izkoriščajo tehničnih ranljivosti sistemov, temveč zavajajo uporabnike, da sami sprožijo ali potrdijo⁵ plačilne transakcije, kar se odraža tudi v strukturi obravnavanih primerov in potrjuje premik težišča goljufij k pristopom, ki temeljijo na vedenjskih in psiholoških prijemih ter dobrem poznavanju postopkov zaznavanja in obravnave goljufij na strani ponudnikov plačilnih storitev. Navedene trende potrjujejo tudi podatki SI-CERT o incidentih v obdobju 2016–2025 (Slika 1).



Slika 1: Obravnavani incidenti 2016 – 2025, Si-Cert (SI-CERT, 2026)

³ European Banking Authority and European Central Bank (2025): "Manipulation of the payer accounted for more than half of the total value of fraudulent credit transfers."

⁴ ENISA (2025): "Based on the analysis of the dataset, social engineering tactics remain the primary entry point for threat actors, with phishing (including vishing, malspam, and malvertising) accounting for about 60% of observed cases."

⁵ European Banking Authority (2025): "Payment fraud is still the most significant issue for EU consumers as a result of new types of fraud such as 'Authorised Push Payment' (APP) fraud, where the payer is manipulated into making a payment to the fraudster."

3. PREPOZNAVA KLJUČNIH PODROČIJ ZA IZBOLJŠANJE VARNOSTI E-PLAČIL IN PREPREČEVANJE PLAČILNIH GOLJUFIJ

DS varnost je v obdobju med letoma 2024 in 2026 na podlagi poglobljene analize trendov in ugotovitev, izkušenj iz prakse, aktualnih goljufij v lokalnem okolju ter obstoječih praks njihove obravnave prepoznala potrebo po bolj usklajenem in sistematičnem pristopu⁶ k obravnavi varnosti elektronskih plačil in z njimi povezanih digitalnih storitev. V nadaljevanju so predstavljeni ukrepi, ki naslavljajo najbolj pereča področja ter predstavljajo podlago za bolj sistematično, poenoteno in učinkovito naslavljanje groženj, kar je nujno glede na naraščajoči trend uspešnih goljufij⁷ in njihovo vse večjo kompleksnost⁸.

Kot strokovna podlaga za oblikovanje izhodišč analize so služili dokumenti Eurosystem Comprehensive Payments Strategy (ECB, 2026), Report from the ERPB Working Group on Fraud Prevention (ERPB, 2024) ter Report on Payment Fraud (EBA & ECB, 2025). Vsi ti viri enotno poudarjajo, da je uspešno preprečevanje goljufij mogoče le skozi usklajen in na podatkih temelječ pristop⁹.

DS varnost je identificirala naslednja ključna področja, za katera v nadaljevanju predlaga konkretne ukrepe:

- varnost e-plačilnih in finančnih aplikacij ter prodajnih mest: smernice za tehnično zaščito e-aplikacij, uvajanje naprednih varnostnih paketov za uporabnike ter zagotavljanje pričakovane ravni varnosti na prodajnih mestih;
- usklajen odziv na kibernetske grožnje in izmenjava podatkov: enoten nacionalni protokol za takojšen in usklajen odziv na grožnje, incidente in vzpostavitev okvira za sprotno deljenje informacij o goljufijah in goljufih;
- ozaveščanje in opismenjevanje: vzpostavitev nacionalne platforme za sistematično dvigovanje digitalne pismenosti prebivalstva ter naslavljanje psiholoških vidikov goljufij (družbeni inženiring);
- nacionalna odpornost in podpora državljanom in podjetjem: Razvoj državnih orodij za kibernetsko odpornost, temeljni varnostni ukrepi za podjetja.

4. VARNOST E-PLAČILNIH APLIKACIJ IN PRODAJNIH MEST

Varnost elektronskih plačilnih aplikacij in prodajnih mest je ključna za zaupanje v digitalna plačila, saj se goljufije vse bolj izvajajo v digitalnih in oddaljenih kanalih ter vključujejo zlorabo uporabniških dostopov in potrjevanja transakcij¹⁰ (EBA & ECB, 2025). Hkrati napadi vse pogostejše temeljijo na socialnem inženiringu, ribarjenju (phishing) in manipulaciji uporabnikov¹¹ (ENISA, 2025), kar povečuje kompleksnost groženj in zahteva širši pristop k varnosti.

⁶ ERPB (2024): "Fraud prevention initiatives need to mobilize all relevant actors from the local, national and EU level in a collaborative way where stakeholders responsibilities are clearly defined."

⁷ EBA & ECB (2025): "This represents a year-on-year increase of EUR 602 million or 17% from 2023 to 2024."

⁸ ERPB (2024): "As elaborated below, the digitalization of services in recent years, notably accelerated by the COVID-19 pandemic, has introduced increased risks in the form of new kinds of fraud and fraud techniques."

⁹ ECB (2026): "strengthening Europe's strategic autonomy and resilience" and "fostering an integrated and innovative payments ecosystem."

¹⁰ EBA & ECB (2025): "payment fraud is still the most significant issue for EU consumers as a result of new types of fraud such as 'Authorised Push Payment' (APP) fraud, where the payer is manipulated into making a payment to the fraudster."

¹¹ ENISA (2025): "Phishing remains the dominant intrusion vector and is evolving through techniques used in large-scale campaigns."

Analize regulativnih organov opozarjajo tudi na razdrobljenost pristopov, vključenost velikega števila različnih deležnikov ter nujno potrebo po bolj usklajenem delovanju in standardizaciji varnostnih praks v celotnem finančnem in plačilnem ekosistemu¹² (ERPB, 2024). Uporabnik pri tem postaja ključni dejavnik tveganja, saj znaten del goljufij nastane kot neposredna posledica njegove manipulacije ali nevednosti, ki vodi v prostovoljno potrditev goljufivih transakcij.

Na tej podlagi se kot ključna področja za prihodnje usmeritve za zagotavljanje varnosti na strani ponudnikov plačilnih storitev in prodajnih mest prepoznavajo:

- smernice za razvoj varnih in uporabniku prijaznih e-plačilnih aplikacij;
- opolnomočenje uporabnikov s sodobnimi varnostnimi paketi in aktivnim upravljanjem osebnih tveganj;
- spodbujanje varne in odgovorne uporabe spletnih, mobilnih in kartičnih plačilnih storitev skozi usklajeno ozaveščanje uporabnikov;
- zagotavljanje pričakovane in standardizirane ravni varnosti na prodajnih mestih.

4.1. Smernice za razvoj varnih in uporabniku prijaznih e-plačilnih aplikacij

Različni pristopi k zasnovi varnosti spletnih in mobilnih plačilnih aplikacij se v praksi odražajo v neenotni ravni zaščite digitalnih plačilnih kanalov ter nerazumevanju uporabnikov. V tem kontekstu se odpira potreba po oblikovanju skupnega okvira varnostne zasnove, katerega cilj je krepitev in vzpostavitev primerljive ravni zaščite ter hkrati omogočanje poenotenega pristopa k varnostnemu ozaveščanju uporabnikov na tem področju.

V nadaljevanju so navedeni primeri področij in možnih pristopov, ki lahko služijo kot izhodišče za oblikovanje skupnega okvira:

- Mobilne plačilne aplikacije: preprečevanje zajema zaslona in delovanja ob aktivnem klicu ter sejah oddaljenega dostopa. Zaznavanje zlonamerne programske opreme, škodljivih procesov, aktivnih sej in klicev ter drugih varnostnih tveganj s telemetrijo. Omejitev naprav s korenskim dostopom (root/jailbreak) ter postopno opuščanje podpore zastarelim operacijskim sistemom. Poenotena varnostna obvestila in opozorila uporabnikom.
- Spletne plačilne aplikacije: zaznavanje anomalij in škodljivih vzorcev delovanja z dinamičnim, tveganjem prilagojenim potrjevanjem transakcij. Nadzor nad varnostnimi mehanizmi ter prilagajanje ali omejevanje storitev ob zaznanih grožnjah. Poenotena varnostna obvestila in opozorila uporabnikom.
- Uporabniške omejitve storitev: možnost omejevanja funkcionalnosti, transakcijskih limitov, prometa in geografskih območij izvajanja. Začasna ali trajna blokada digitalnih kanalov z možnostjo deblokade izključno ob osebnem obisku poslovalnice.
- Poenotena opozorila in varnostna obvestila: obvezno obveščanje ob vstopu v kanal, potrjevanju plačil, spremembi kontaktnih podatkov ali pooblastil, sklenitvi novih produktov, spremembi transakcijskih limitov in drugih tveganjih dejanjih.

¹² ERPB (2024): "Fraud prevention initiatives need to mobilize all relevant actors from the local, national and EU level in a collaborative way where stakeholders responsibilities are clearly defined."

- Pogojeno izobraževanje v digitalnih kanalih: periodično ozaveščanje o varni uporabi storitev, potrditev razumevanja varnostnih priporočil pred aktivacijo ter možnost omejitve funkcij do zaključka ključnih izobraževalnih korakov.

4.2. Varnostni paketi in upravljanje tveganj s strani uporabnika

Ponudniki omogočijo uporabnikom izbiro med različnimi varnostnimi paketi pri uporabi plačilnih storitev, ki odražajo različno raven funkcionalnosti, razpoložljivih storitev in zaščitnih mehanizmov ter opolnomočijo uporabnike k zavestnemu upravljanju lastne izpostavljenosti varnostnim tveganjem. Takšen pristop omogoča, da uporabniki glede na svoje znanje, izkušnje in potrebe izberejo ustrezen način uporabe plačilnih storitev.

Pri tem bi lahko bolj konservativni oziroma digitalno manj pismeni uporabniki izbrali pakete z višjo stopnjo varnosti, v katerih so tvegane plačilne funkcionalnosti privzeto omejene ali onemogočene, omogočeno pa je osnovno in varno poslovanje, na primer plačevanje računov domačim podjetjem. Naprednejši uporabniki, ki so bolj seznanjeni s tveganji, pa bi lahko izbrali pakete z nižjo stopnjo varnostnih omejitev, ki omogočajo bolj fleksibilno in enostavno uporabo plačilnih in drugih storitev.

4.3. Usmeritve za varno in odgovorno uporabo plačilnih storitev

Prepoznana je potreba poenotenja ravnanj in dobrih praks ponudnikov plačilnih storitev, s čimer se uporabnikom zagotovi jasna in razumljiva navodila za varno in odgovorno uporabo spletnih, mobilnih in kartičnih storitev. Takšen pristop omogoča tudi enotno ozaveščanje javnosti. Skupne usmeritve bi primarno nasloville:

- opredelitev pričakovanega ravnanja pri uporabi digitalnih plačilnih kanalov, vključno z ravnanjem ob spremembah nastavitvev, limitov in pooblastil;
- opredelitev ravnanja v zvezi z elementi digitalne identitete ter metodami avtentikacije in potrjevanja transakcij;
- poenotene usmeritve glede ravnanja z bančnimi karticami, vključno z uporabo kartic, upravljanjem PIN-ov in ravnanjem na bankomatih;
- opredelitev pričakovanega ravnanja ob prejemu komunikacij, povezanih s plačilnimi storitvami, ter preverjanja njihove pristnosti;
- opredelitev ravnanja ob zaznavi ali sumu goljufije, vključno z obveznostjo pravočasnega obveščanja ponudnika plačilnih storitev;
- opredelitev odgovornega ravnanja z napravami, ki se uporabljajo za izvajanje plačilnih storitev.

4.4. Zagotavljanje pričakovanega nivoja varnosti za prodajna mesta

Ukrep vzpostavlja okvir za pregled obstoječih varnostnih zahtev in praks na prodajnih mestih ter za opredelitev enotnega minimalnega nabora varnostnih zahtev in mehanizmov nadzora njihovega izvajanja, z namenom zmanjševanja izpostavljenosti plačilnim goljufijam:

- vzpostavitev okvira za pregled in posodobitev obstoječih minimalnih tehničnih in organizacijskih varnostnih zahtev za prodajna mesta ter mehanizmov za redno preverjanje njihove ustreznosti, ažurnosti in izvajanja;

- poenoteni varnostni protokoli za sprejem elektronskih plačil na fizičnih in spletnih prodajnih mestih (POS-terminali, QR-plačilne storitve ter rešitve za sprejem plačil na spletnih prodajnih mestih);
- zahteva po rednem in ciljno usmerjenem izobraževanju zaposlenih na prodajnih mestih o plačilnih storitvah, tipičnih goljufijah in varnem ravnanju v plačilnih procesih;
- povezovanje obstoječih zahtev (npr. kartične sheme, industrijski standardi) v enoten okvir, ki omogoča primerljivo raven varnosti in učinkovitejšo obravnavo incidentov;
- redno izobraževanje zaposlenih na prodajnih mestih o različnih plačilnih storitvah, ki so na voljo ter varnem rokovanju.

5. ODZIV, OBRAVNAVE IN IZMENJAVA PODATKOV MED DELEŽNIKI

Ugotovitve iz prakse kažejo, da so obstoječi odzivni mehanizmi in komunikacijske poti med akterji razdrobljeni. Težavo dodatno stopnjuje dejstvo, da so ključni akterji (npr. ponudniki gostovanj lažnih spletnih strani) pogosto v tujini in neodzivni, kar bistveno podaljšuje odzivne čase, vključno z umiki zlonamernih vsebin. Za učinkovito zmanjševanje plačilnih goljufij je zato nujen prehod na usklajen nacionalni model, ki povezuje tehnično obrambo, operativne protokole in zakonito deljenje informacij, kar izrecno podpirajo tudi uradne analize evropskih regulatorjev v svojih poročilih (EBA & ECB, 2025), (ERPB, 2024) ter na globalni ravni tudi Združeni narodi (Global Fraud Summit, 2026)¹³.

DS varnost kot ključne korake za reševanje teh izzivov prepoznava naslednje nujne ukrepe:

- poenoteni ukrepi odziva na nacionalni ravni;
- vzpostavitev nacionalnega okvira za izmenjavo podatkov o plačilnih goljufijah;
- protokol o obravnavi plačilnih goljufij na nacionalni ravni.

5.1. Poenoteni tehnični ukrepi odziva na nacionalnem nivoju

Trenutni neenotni pristopi k naslavljanju zlorab komunikacijskih in spletnih kanalov ter odsotnost centraliziranega tehničnega odziva se v praksi odražajo v omejeni učinkovitosti omejevanja plačilnih goljufij in lažnega predstavljanja na nacionalni ravni. V tem kontekstu se odpira potreba po oblikovanju skupnega okvira nacionalnih ukrepov in sistemskih rešitev, katerega cilj je v tesnem sodelovanju s ponudniki elektronskih komunikacij vzpostaviti usklajeno, hitro in tehnično učinkovito obrambo pred tovrstnimi zlorabami sodobnih komunikacijskih kanalov.

V nadaljevanju so navedena ključna področja in ukrepi, ki lahko služijo kot izhodišče za oblikovanje tega skupnega okvira:

¹³ ERPB (2024): "The scope of fraud, its complexities, and the range of actors it involves does not yet fall fully under the mandate of any specific organisation."
EBA & ECB (2025): "Most payment transactions were domestic, but the majority of card payment fraud as well as a large share of credit transfer and direct debit fraud were cross-border."
UN (2026): "The timely, secure and lawful sharing of data and actionable information by all relevant actors, with due regard to data protection and privacy, is key to an effective fraud response."

- vpeljava DNS-usmerjanja na opozorilne strani: ob zaznavi in prijavi zlonamernih spletnih povezav (npr. phishing strani) operaterji na ravni omrežja izvedejo preusmeritev uporabnika na enotno opozorilno stran. Uporabniku se prikaže opozorilo o nevarnosti, pri čemer se ohrani možnost dostopa na lastno odgovornost (razen v primerih, ko je vsebina pri ponudniku gostovanja že trajno odstranjena);
- nadzor nad integriteto identifikacije kličočega (CLI): Vzpostavitev tehničnega nadzora na ravni operaterjev, ki omogoča preverjanje ujemanja identitete kličočega. Sistem ob zaznavi neujemanja ali ponarejanja številke (t.i. CLI spoofing) avtomatsko opozori uporabnika s sistemskim sporočilom ali sumljiv klic/SMS blokira;
- ukinitve anonimnih mobilnih števil: Zakonodajna naslovitev vprašanja predplačniških SIM-kartic brez identifikacije lastnika, ki predstavljajo glavno orodje za izvajanje lažnega predstavljanja in investicijskih goljufij, ter uvedba njihove postopne in popolne ukinitve na nacionalni ravni.

Pogoji za učinkovito operacionalizacijo ukrepov:

- Operativne postopke in protokole za takojšnje tehnično omejevanje zlonamernih vsebin je treba strogo ločiti od standardnih postopkov prijave, zakonskega poročanja o večjih incidentih ter dolgotrajnega obveščanja o ranljivostih.
- Določitev enotne točke za prijavo zlonamernih vsebin: formiranje osrednjega nacionalnega vozlišča (v okviru SI-CERT, URSIV ali z ustanovitvijo namenskega finančnega CERT-a). Na to točko se nemudoma javljajo zaznane goljufije, od tam pa se avtomatizirano in v realnem času sprožijo ukrepi za omejevanja dostopa do lažnih spletnih mest pri vseh telekomunikacijskih operaterjih hkrati.
- Oblikovanje ustreznih pravnih okvirov, ki bodo telekomunikacijskim operaterjem zakonsko omogočili in naložili izvajanje sorazmernih, avtomatiziranih ter hitrih ukrepov omejevanja dostopa do lažnih spletnih strani ter preprečevanja lažnega prikazovanja telefonskih števil (klicev in SMS-sporočil).

5.2. Nacionalni protokol za celovito obravnavo plačilnih goljufij

Ugotovitve kažejo, da trenutni postopki obravnave goljufij, zlasti ravnanja in zadržanje sredstev, niso usklajeni med različnimi deležniki v plačilni infrastrukturi ter med deležniki na nacionalni ravni. Enoten protokol na nacionalni ravni bi predstavljal okvir za učinkovito obravnavo plačilnih goljufij z namenom zagotavljanja hitrega odziva, jasne razdelitve vlog ter usklajenega ravnanja bank, hranilnic, pristojnih institucij in drugih deležnikov.

Smernice za oblikovanje nacionalnega protokola naj obsegajo naslednja področja:

- poenotenje postopkov in ravnanj ob zaznavi plačilnih sumljivih transakcij in goljufij;
- jasna opredelitev vlog, odgovornosti in komunikacijskih poti med bankami, komitenti ter pristojnimi institucijami (Policija, UPPD, SI-CERT);
- opredelitev ravnanja in rokov pri zadržanju sredstev ter omejevanju poslovanja ob sumu goljufije, vključno z uporabo UAN;
- jasna pravna podlaga za zadržanje sredstev in blokade (računi, uporabniki) ter usklajena praksa njihove uporabe;
- izboljšanje in formalizacija medbančne komunikacije v posameznih primerih goljufij;

- naslovitev postopkov čezmejne izmenjave podatkov ter ravnanja pri zadržanju sredstev pri tujih bankah in finančnih posrednikih.

5.3. Vzpostavitev nacionalnega okvira za izmenjavo podatkov o plačilnih goljufijah

Prepoznana je potreba po vzpostavitvi nacionalnega okvira ter identifikaciji oziroma vzpostavitvi ustrezne pravne podlage za usklajeno, pravočasno in zakonito izmenjavo podatkov o plačilnih goljufijah in goljufijah med relevantnimi deležniki, ob jasni razmejitvi vrst podatkov, namena njihove uporabe ter kroga upravičenih prejemnikov, z namenom učinkovitega preprečevanja, zaznavanja in omejevanja goljufij na nacionalni ravni:

- izmenjava tehničnih podatkov in indikatorjev ogroženosti (IOC/IOF) med ponudniki plačilnih storitev, operaterji elektronskih komunikacij, SI-CERT in drugimi relevantnimi subjekti, ob uporabi standardiziranih platform (npr. MISF) ter poveztivosti z evropskimi pobudami (npr. iniciativa FRIDA), za hitro zaznavo in omejevanje goljufij;
- izmenjava podatkov o potrjenih plačilnih goljufijah in prizadetih komitentih med bankami in drugimi ponudniki plačilnih storitev, omejena na obravnavo posameznih primerov in preprečevanje ponovitve goljufij, ob jasno opredeljenih pogojih in varovalkah za zaščito zakonitih uporabnikov;
- opredelitev pravil upravljanja izmenjave podatkov, vključno z namenom uporabe, ravnmi dostopa, sledljivostjo ter postopki za obravnavo napačnih zaznav (false positive), za zagotovitev zaupanja in pravne varnosti;
- vzpostavitev registra visoko rizičnih strank (po vzoru zavarovalniškega sistema SIS), ki sodelujejo v plačilnih goljufijah (npr. denarne mule).

6. NACIONALNA PLATFORMA ZA OZAVEŠČANJE IN DIGITALNO OPISMEJENJE

DS Varnost na podlagi izmenjanih izkušenj iz prakse ugotavlja, da razdrobljeno in neusklajeno ozaveščanje prinaša skromne rezultate, saj povzroča zasičenost uporabnikov z informacijami. Za prehod od informacijskega hrupa (Sharma, 2025)¹⁴ k dejanski odpornosti se izrecno zagovarja vzpostavitev centralizirane, panožne in medsektorske platforme, ki prevzame koordinacijo ozaveščanja, opozarjanja in izobraževanja ter zagotavlja enoten, usklajen in preverjen prenos informacij do uporabnikov (Euroconsumers, 2026)¹⁵.

Priporočamo, da se za večjo preglednost in dostopnost za vse deležnike in uporabnike centralizira zbiranje gradiv in obvestil na enem mestu, na primer na spletni strani Ministrstva za finance, ki je v

¹⁴ "In today's hyperconnected world, constant notifications, information overload, and the pressure to remain online create a state of cognitive fatigue that weakens concentration, reduces productivity, and heightens stress levels."

"Digital drain also increases vulnerability to cybercrime, as fatigue lowers attention and critical judgment, making individuals more likely to fall prey to scams and online risks."

¹⁵ Euroconsumers (2026): "National Anti-Scam Centres represent a structural response that matches the sophistication and cross-border nature of modern fraud." okument takim centrom pripisuje vlogo osrednje koordinacijske točke za prijavo goljufij, podporo žrtvam, izmenjavo informacij, usklajevanje tehničnega in medsektorskega odziva ter izvajanje enotnih preventivnih, opozorilnih in ozaveševalnih aktivnosti.

pripravi v okviru Nacionalnega programa finančnega opismenjevanja (NFPO) (Vlada Republike Slovenije, 2025) in bo vključevala tudi vsebine s področja varnosti elektronskih plačil.

Namen nacionalne platforme je vzpostaviti enoten, zaupanja vreden okvir o vsebinah za preprečevanje goljufij pri plačilih, socialnem inženiringu ter varni uporabi digitalnih storitev in digitalnih identitet, ki omogoča usklajeno, pravočasno in enotno obveščanje vseh ciljnih skupin:

- centraliziran nabor preverjenih vsebin in priporočil, ki jih dosledno uporabljajo vsi deležniki (regulatorji, SI-CERT, Policija, ZBS, ZPS, operaterji, GZS/OZS);
- vključitev digitalne pismenosti in varnega spletnega vedenja v formalne in neformalne izobraževalne programe (šole, univerze, delodajalci, javna uprava), s poudarkom na ranljive ciljne skupine (mladi, starejši; sedaj izvajajo MF, MDP, ZPS, BS);
- povezovanje platforme z nacionalnimi viri incidentov in opozoril (npr. SI-CERT, URSIV), kar omogoča sprotno informiranje in enotno usmerjanje uporabnikov v primeru zaznanih groženj;
- usklajene in poenotene nacionalne komunikacijske kampanje ter mehanizmi za zgodnje odzivanje za obveščanje javnosti (push/portal/SMS/e-pošta) o aktualnih grožnjah, goljufijah in preventivnih ukrepih.

7. DODATNI UKREPI NA NACIONALNEM NIVOJU

Narava kibernetских groženj se hitro spreminja, tehnična zaščita infrastrukture pa je neločljivo povezana s človeškim dejavnikom, ta sklop opredeljuje štiri dodatna področja, ki jih je DS varnost prepoznala kot pomembne gradnike, ki jih je smiselno celovito nasloviti na nacionalni ravni, kar potrjujejo tudi ugotovitve analiz pristojnih institucij (ERPB, 2024), (ENISA, 2024) ter strateška usmeritev krovne Uredbe EU eIDAS 2 (EU, 2024)¹⁶.

7.1. Razvoj nacionalnih virov groženj in orodij za digitalno odpornost

Posamezniki in manjša podjetja varnostnega vidika pogosto ne naslavlajo s potrebno skrbnostjo. Da bi dvignili raven njihove varnostne drže in jih spodbudili k redni uporabi zaščitnih orodij, je priporočljivo vzpostaviti jasne smernice, ki bodo podprte z dostopnimi, osnovnimi varnostnimi rešitvami in storitvami za pokrivanje ključnih tveganj.

V nadaljevanju so navedena ključna področja in možni pristopi, ki lahko služijo kot izhodišče za oblikovanje predlaganega:

- Konsolidacija nacionalnih in mednarodnih virov groženj (Threat Intelligence)¹⁷: vzpostavitev lokalno prilagojenih virov (podatkovni viri, RSS) z naprednimi indikatorji ogroženosti (IOC, hash vrednosti škodljive kode), kar je ključno za delovanje DNS-preusmerjanja v točki 3.5. Vključuje integracijo z

¹⁶ ERPB (2024): "The scope of fraud, its complexities, and the range of actors it involves does not yet fall fully under the mandate of any specific organisation."

ENISA (2025): "Overall, the distribution underscores that while phishing dominates the threat landscape, technical exploits, malware delivery mechanisms and insider risks remain meaningful concerns."

¹⁷ ERPB (2024): "There is a need to promote and support the exchange of information and share actions implemented against fraud among all relevant national actors identified by the WG."

evropskimi platformami (CSIRT), zakup komercialnih virov groženj ter obvezno uporabo teh podatkov v kritični infrastrukturi in pri operaterjih za zaščito končnih uporabnikov.

- Nacionalna platforma za verifikacijo digitalnih vsebin: vzpostavitev namenskega spletnega mesta za regijsko prilagojeno preverjanje legitimnosti povezav, e-sporočil in priponk. Platforma vključuje register varnih slovenskih domen (npr. spletnih bank), analizo metapodatkov domen (starost, država, lastnik, ocena sumljivosti), napredno analizo z državno AI ter možnost neposredne prijave novih zaznanih goljufij.
- Namenska zaščitna programske opreme za končne naprave: razvoj nacionalne mobilne/namizne aplikacije (ali integriranega SDK), ki deluje kot sistemska požarna pregrada z DNS-filtriranjem na nivoju naprave. Rešitev blokira prenos zlonamernih vsebin, opozarja na sumljive povezave v SMS-sporočilih, e-pošti in kodah QR-plačilnih storitev ter omogoča povezavo s komercialnimi antivirusnimi rešitvami za osnovno EDR-zaščito in telemetrijo.
- Sistemsko alarmiranje in paketne varnostne storitve za končne uporabnike: vzpostavitev avtomatiziranega sistema obveščanja o aktivnih phishing kampanjah (obvezna push/e-poštna obvestila za kritično infrastrukturo, priporočljiva za podjetja in posameznike). Ponudba modularnih paketov (brezplačni osnovni in plačljivi napredni), ki vključujejo upravljanje gesel in MFA (povezava z e-OI), oblačno shrambo za varnostne kopije, preverjanje sistemskih ranljivosti (CVE > 8.0), zaščito prometa prek nacionalnega e-poštnega prehoda, skripte za utrjevanje sistemov ter tehnično podporo.

7.2. Usmeritve za pripravo minimalnih tehničnih ukrepov in kontrol za pravne subjekte

Razpršene varnostne prakse med pravnimi subjekti z omejenimi kadrovskimi in finančnimi kapacitetami večajo izpostavljenost celotnega sistema in tveganja za plačilne goljufije. Smiselno je oblikovati enoten okvir minimalnih tehničnih ukrepov in kontrol, ki bo zagotovil primerljivo osnovno raven informacijske varnosti, predvsem pri zavezancih po ZInfV-1.¹⁸ Te usmeritve bodo služile kot primer dobre prakse za prenos po dobavnih in storitvenih verigah, kar bo okrepilo obvladovanje tveganj tudi na nacionalnem nivoju.

Izhodišča za oblikovanje tega skupnega okvira kontrol obsegajo:

- Smernice in obvezna uporaba skupnih virov groženj: okvir mora jasno opredeliti tehnične kontrole ter določiti obvezno integracijo skupnih varnostnih virov in orodij, predlaganih v točki 5.2. To bo služilo kot dopolnitev ali stroškovno dostopna alternativa komercialnim rešitvam za subjekte brez obstoječe zaščite.
- Vzpostavitev in nudenje podpore pri upravljanju nujenih varnostnih rešitev: zagotoviti je treba enotno tehnično platformo z naborom osnovnih zaščitnih rešitev ter hkrati vzpostaviti sistemsko podporo pri njihovem vsakodnevnem upravljanju. Ta pomoč je namenjena izvajalcem bistvenih storitev in manjšim podjetjem, ki nimajo lastnih kadrovskih kapacitet za celovito upravljanje informacijskih tveganj.

¹⁸ ENISA (2025): "Vulnerability exploitation remains a cornerstone of initial access (21.3%), with widespread campaigns rapidly weaponising them within days of their disclosure—underscoring the need to ensure patch availability and to implement and enforce basic measures for cyber hygiene."

7.3. Obravnava in podpora psihološkega vidika plačilnih goljufij

Analize in primeri iz prakse kažejo, da klasični tehnični ukrepi, varnostna opozorila in splošno ozaveščanje sami po sebi niso dovolj za preprečevanje naprednih goljufij, kot so investicijske in romantične goljufije, lažni klici o nesrečah družinskih članov ter lažno predstavljanje banke ali tehnične podpore (EBA & ECB, 2025) in (ERPb, 2024). Storilci z uporabo družbenega inženiringa žrtve potisnejo v stanje psihološkega ujetništva, v katerem uporabniki slepo zaupajo storilcem, prostovoljno razkrijejo osebne podatke ter predajo dostope do plačilnih kanalov, medtem ko standardna opozorila zavestno ignorirajo.

Na nacionalni ravni je treba uvesti točko, na katero se lahko žrtve in njihovi svojci obrnejo za pravno pomoč ter psihološko podporo (Global Fraud Summit, 2026)¹⁹. Hkrati je nujno vzpostaviti usmerjena izobraževanja za prepoznavanje potencialnih žrtev in potrebnih ravnanj.

7.4. Poenotenje digitalne identitete in uporabniške izkušnje

Večina dostopov do plačilnih aplikacij in digitalnih storitev poteka z uporabo digitalnih identitet, ki jih zagotavljajo predvsem slovenski ponudniki, kar še dodatno izpostavlja pomen njihove enostavne, razumljive in enotne uporabe.

Obstoječi postopki in uporabniška izkušnja digitalnih identitet so razdrobljeni, neenotni in za uporabnike težko razumljivi, kar se kaže v težavah uporabnikov pri namestitvi, ponastavitvi ali menjavi identitete. Postopki niso intuitivni, uporabniki ne razumejo delovanja niti samega koncepta digitalne identitete, zaradi česar so nezaupljivi pri uporabi in posledično tudi bolj dovzetni za zlorabe.

DS varnost zato predlaga poenotenje postopkov in uporabniške izkušnje digitalne identitete med nacionalnimi ponudniki z namenom poenostavitve uporabe ter izboljšanja razumljivosti in zaupanja uporabnikov, pri čemer predstavlja uvedba nacionalne digitalne denarnice (EUDIw) izhodišče za optimizacijo in poenotenje pristopov med ponudniki. Evropska digitalna denarnica omogoča enotno upravljanje, dostop in deljenje identifikacijskih podatkov ter izboljšuje postopke identifikacije in avtentikacije na enoten, varen in zanesljiv način v celotni EU (ENISA, 2024)²⁰.

8. NACIONALNA KOORDINACIJA IDENTIFICIRANIH UKREPOV

Delovna skupina za varnost ugotavlja, da predlagani ukrepi ter prepoznane možnosti uskladtve in poenotenja postopkov odziva ob goljufijah in drugih kibernetских tveganjih jasno kažejo, da posamezne aktivnosti same po sebi ne morejo doseči želenih učinkov brez usklajene koordinacije na nacionalni ravni. Ukrepi in rešitve, ki naslavljajo tehnične in postopkovne vidike, vključno z dvigom informacijske ozaveščenosti in digitalne pismenosti na nacionalni ravni, so medsebojno povezani ter presegajo

¹⁹ UNODC (2026): " Supporting victims of fraud is essential for rebuilding trust and confidence, reducing further harm, learning from their experiences, and facilitating their cooperation for an effective criminal justice response, enabling the continuous improvement of prevention strategies, awareness efforts and policy responses."

²⁰ ENISA (2024): " ENISA (2024): "EUDI Wallets allow storing, accessing and sharing of personal identification data and documents ... Online identification and authentication processes will be improved and address longstanding barriers in a common, safe and reliable way across Europe."

pristojnosti in vpliv posameznih deležnikov. Njihova učinkovita uresničitev zato zahteva usklajen pristop, ki omogoča celovito razumevanje tveganj, koordinacijo ravnanj ter dosledno izvajanje dogovorjenih usmeritev in ukrepov. V skladu s svojim mandatom je Delovna skupina za varnost prispevala k poglobljenemu razumevanju zatečenega stanja na področju varnosti elektronskih plačil ter pripravila strokovne podlage in predloge za naslovitev identificiranih sistemskih vrzeli. Ena ključnih ugotovitev DS Varnost je, da obstoječe stanje odpira potrebo po nadaljnjem razmisleku o ustreznih okvirih za okrepljeno in bolj usklajeno naslavljanje teh izzivov na nacionalni ravni.

Navedeno odpira potrebo po vzpostavitvi nacionalnega telesa, ki bi vključevalo ključne deležnike iz gospodarstva in finančne industrije ter pristojne državne organe, odgovorne za zakonodajni, nadzorni in operativni vidik obravnave ter odziva na kibernetika tveganja. Ta tveganja se prenašajo po celotni komunikacijski, informacijski in plačilni infrastrukturi ter se ne naslavlajo zgolj s posameznimi varnostnimi rešitvami ponudnikov elektronskih plačilnih storitev.

Na tej podlagi se utemeljuje tudi potreba po identifikaciji pristojnega organa, ki bi vodil vzpostavljeno telo ter imel jasno opredeljena pooblastila, odgovornosti in operativne pristojnosti za koordinacijo, izvajanje in nadaljnji razvoj identificiranih ukrepov na nacionalni ravni.

9. ANALIZA POTREB IN ZAHTEV ZA VZPOSTAVITEV NACIONALNEGA FORUMA

Ugotovitve DS varnost kažejo, da je za operacionalizacijo in nadaljnji razvoj ukrepov, skladno z razvojem kibernetičnih tveganj na področju elektronskih plačil in digitalnih storitev, potrebna vzpostavitev pristojnega telesa na nacionalni ravni.

Ustanovitev Nacionalnega foruma oziroma ustreznega koordinacijskega organa za obravnavo goljufij na področju elektronskih plačil bi zagotovila centralno platformo za razpravo, posvetovanje, sodelovanje ter izmenjavo informacij in stališč, namenjenih celostni obravnavi varnostnih vidikov elektronskih plačil in povezanih storitev. Pristojno telo bi skrbelo za razvoj nacionalnih smernic, pravne podlage, postopkov in orodij za odziv in preprečevanje goljufij ter hkrati zagotavljalo učinkovito koordinacijo med deležniki z namenom enotnega ozaveščanja in izobraževanja na nacionalni ravni.

9.1. Naloge, pristojnosti in sestava Forum

Za uspešen prenos strateških usmeritev v neposredno prakso predlagani model organiziranosti deluje na dveh ravneh:

- Nacionalni forum je krovno telo na strateški ravni, ki spremlja makro trende, določa prioritete, obravnava zakonodajne ureditve in identificira potrebe po nadgradnji ter skrbi za razvoj nacionalnih smernic, postopkov in orodij za odziv, omejevanje tveganj ter preprečevanje goljufij.
- Operativno raven pa predstavljata dve delovni podskupini znotraj Forum, ki prenašata usmeritve v operativno. Prva skupina (Skupina za operativni razvoj odpornosti) je usmerjena v tehnično in sistemsko izvedbo ukrepov, druga skupina (Skupina za ozaveščanje in izobraževanje) pa zagotavlja učinkovito koordinacijo med deležniki z namenom enotnega ozaveščanja in izobraževanja na nacionalni ravni.

9.1.1. Nacionalni forum za varnost elektronskih plačil

Nacionalni forum predstavlja osrednjo koordinacijsko in posvetovalno platformo na nacionalni ravni. Njegove ključne naloge so:

- spremljanje trendov na področju varnosti elektronskih plačil in goljufij;
- opredeljuje prioritete ter spodbuja aktivnosti deležnikov;
- obravnava zakonodajne ureditve in pripravlja relevantne predloge sprememb;
- izmenjuje informacije o tveganjih, trendih in zaznanih pojavih med deležniki;
- opredeljuje, oblikuje in komunicira skupna stališča;
- razvija dobre prakse ter oblikuje in predlaga ukrepe za zmanjševanje tveganj ter spremlja njihovo učinkovitost;
- oblikuje predloge, ki presegajo nacionalne okvire;
- spremlja izvajanje dogovorjenih aktivnosti deležnikov.

9.1.2. Skupina za operativni razvoj odpornosti

Skupina za razvoj nacionalnega odziva deluje v okviru Foruma in je usmerjena v operacionalizacijo identificiranih ukrepov. Njene naloge vključujejo:

- analizo predlogov in usmeritev Foruma;
- pripravo predlogov možnih ukrepov in potrebnih aktivnosti skupaj z načrtom njihove uvedbe;
- koordinacijo uvajanja identificiranih ukrepov na nacionalni ravni;
- identifikacijo obstoječe pravne podlage ter pripravo predlogov za njeno dopolnitev ali vzpostavitev, kjer je to potrebno.

9.1.3. Skupina za razvoj nacionalnih programov za ozaveščanja in izobraževanj iz obravnavanih področij

Skupina zagotavlja učinkovito koordinacijo med deležniki z namenom enotnega ozaveščanja in izobraževanja na nacionalni ravni:

- izmenjavo informacij med deležniki (periodični sestanki in obveščanje prek e-kanalov);
- skupno pripravo in izmenjavo gradiv za ozaveščanje;
- koordinacijo širših aktivnosti (skupne kampanje, dogodki, distribucija materialov);
- usklajevanje skupnih obvestil, opozoril ali izjav za javnost, vezanih na temo varnosti elektronskih plačil.

Skupina za ozaveščanje in izobraževanje je odgovorna za usklajevanje in nadgradnjo nacionalnih aktivnosti na področju krepitve digitalne in informacijske pismenosti. Njene naloge vključujejo:

- usklajevanje obstoječih programov ozaveščanja in informiranja (npr. ZPS, SI-CERT, ZBS in drugi);

- razvoj in povezovanje programov izobraževanja in digitalnega opismenjevanja, ki jih izvajajo pristojni organi, izobraževalne institucije in drugi deležniki (npr. MF, MDP, ZBS, komercialni ponudniki);
- vključevanje področja varne uporabe elektronskih plačil v formalne izobraževalne programe, zlasti v sodelovanju z MVI in izobraževalnimi ustanovami.

9.2. Identifikacija deležnikov v Forumu in skupinah

V Nacionalni forum za varnost elektronskih plačil in njegove delovne skupine se vključijo ključni deležniki, katerih vloga, pristojnosti ali delovanje so neposredno povezani z varnostjo elektronskih plačil, obravnavo goljufij ter ozaveščanjem in zaščito uporabnikov.

Seznam identificiranih deležnikov je podrobneje opredeljen v Aneksu 1 tega dokumenta. Deležniki se vključujejo v delovanje Foruma in delovnih skupin glede na pristojnosti.

10. ZAKLJUČEK

Predlagani ukrepi in sistemske usmeritve v tem dokumentu predstavljajo potreben korak naprej k celoviti zaščiti slovenskega plačilnega ekosistema. Analize in izkušnje v praksi jasno potrjujejo, da razdrobljeno delovanje posameznih institucij ne zadošča več za boj proti sodobnim, tehnološko naprednim in psihološko uigranim goljufijam. Učinkovit odziv je mogoč le s preходом na usklajen nacionalni ekosistem, ki povezuje tehnične kontrole, avtomatizirane postopke odziva ter optimizirane protokole ravnanj in izmenjave podatkov med deležniki v plačilni, nacionalni in komunikacijski infrastrukturi.

Uresničitev teh ciljev sloni na treh ključnih stebrih, ki obsegajo:

- (i) hitro blokado zlonamernih vsebin,
- (ii) varno in zakonito izmenjavo podatkov o grožnjah ter goljufijah in
- (iii) gradnjo nacionalne platforme za digitalno ozaveščanje in opismenjevanje.

S tem bomo dolgoročno zmanjšali ranljivost uporabnikov, poenotili delovanje vseh akterjev ter okrepili splošno varnost in zaupanje v elektronske plačilne storitve v Sloveniji.

CITATI IN VIRI

- Global Fraud Summit. (2026). *Call to Action on Combating Fraud & Global Public-Private Partnership Framework against Fraud*. Pridobljeno 10. 6 2026 iz Global Fraud Summit: <https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf>
- EBA & ECB. (15. 12 2025). *2025 REPORT ON PAYMENT FRAUD*. Pridobljeno 5. 6 2026 iz <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf>
- EBA. (marec 2025). *Consumer Trends Report 2024-2025*. Pridobljeno iz European Banking Authority: <https://www.eba.europa.eu/publications-and-media/consumer-trends-report-2024-2025>
- ECB. (2026). *The Eurosystem's comprehensive payments strategy*. Pridobljeno 20. 6 2026 iz <https://www.ecb.europa.eu/press/pubbydate/2026/html/ecb.eurosystemcomprehensivepaymentsstrategy202603.en.html>
- ECP. (February 2025). *Payments Threats and Fraud Trends Report*. Pridobljeno iz European Payments Council: <https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2025-02/EPC162-24%20v2.0%202025%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf>
- ENISA. (24. 9 2024). *EU Digital Identity Wallet: A leap towards secure and trusted electronic identification through certification*. Pridobljeno 10. 6 2026 iz <https://www.enisa.europa.eu/news/eu-digital-identity-wallet-a-leap-towards-secure-and-trusted-electronic-identification-through-certification>
- ENISA. (10 2025). *ENISA THREAT LANDSCAPE 2025*. Pridobljeno 10. 6 2026 iz <https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025.pdf>
- EPC. (10 2024). *2024 Payment Threats and Fraud Trends Report*. Pridobljeno 10. 6 2026 iz https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf
- ERPB. (2024). *Report of the ERPB Working Group on fraud related to retail payments*. Pridobljeno 10. 6 2026 iz https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/21st-ERPB-meeting/Report_from_the_ERPB_Working_Group_on_fraud_prevention.pdf
- EU. (2024). *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Pridobljeno 10. 6 2026 iz <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>
- Euroconsumers. (February 2026). *Response to the Call for Evidence: Action Plan on Fighting Online Fraud*. Pridobljeno iz Euroconsumers: https://www.euroconsumers.org/wp-content/uploads/2026/02/Euroconsumers-Response-to-the-Call-for-Evidence_Action-Plan-on-Fighting-Online-Fraud.pdf
- NSP. (20. 12 2023). Pridobljeno 5. 6 2026 iz Strategija razvoja trga plačil v Sloveniji za obdobje 2024-2028: https://www.bsi.si/storage/uploads/e1345a17-e3d2-4a19-b33c-6940b4430e2a/Strategija_razvoja_trga_placil_v_Sloveniji_2024-2028.pdf
- Sharma, A. (September 2025). *The Digital Drain: Psychological Exhaustion, Social Disruptions, and Online Vulnerabilities*. Pridobljeno iz IOSR Journal of Humanities and Social Science (IOSR-JHSS): <https://iosrjournals.org/iosr-jhss/papers/Vol.30-Issue9/Ser-2/M30090297102.pdf>

SI-CERT. (22. 1 2026). *Spletni seminar SI-CERT poročilo o kibernetiski varnosti 2025*. Pridobljeno 10. 6 2026 iz <https://www.cert.si/spletni-seminar-si-cert-porocilo-o-kibernetiski-varnosti-2025/>

Vlada Republike Slovenije. (30. 1 2025). Pridobljeno 5. 6 2026 iz Nacionalni program finančnega opismenjevanja: <https://www.gov.si/assets/ministrstva/MF/Financni-sistem/DOKUMENTI/Financno-izobrazevanje/Nacionalni-program-financnega-opismenjevanja.pdf>

ANEKS 1: Seznam identificiranih deležnikov foruma in delovnih skupin

1. Državni organi in institucionalni deležniki

Vključitev v delovanje Foruma ter obeh delovnih skupin, glede na pristojnosti)

- Banka Slovenije
- Ministrstvo za finance
- Ministrstvo za pravosodje
- Ministrstvo za vzgojo in izobraževanje
- Urad za preprečevanje pranja denarja
- Uprava Republike Slovenije za javna plačila
- Urad Vlade Republike Slovenije za informacijsko varnost
- SI-CERT
- Policija
- Agencija za komunikacijska omrežja in storitve Republike Slovenije
- Informacijski pooblaščenec

2. Interesna združenja

Vključitev v delovanje Foruma ter skupine za ozaveščanje in izobraževanje:

- Zveza potrošnikov Slovenije
- Združenje bank Slovenije
- Trgovinska zbornica Slovenije
- Gospodarska zbornica Slovenije
- Sekcija operaterjev elektronskih komunikacij

3. Procesorji plačilnih instrumentov

Vključitev v delovanje Foruma ter skupine za razvoj nacionalnega odziva:

- Bankart
- Dinit
- Nexi

4. Plačilne sheme

Vključitev v delovanje Foruma ter skupine za razvoj nacionalnega odziva:

- Visa
- Mastercard
- Karanta