Ko močna avtentikacija ni dovolj: forenzični pogled na bančno goljufijo z oddaljenim dostopom

Boštjan Kežmah, Miha Strehar

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija
bostjan.kezmah@um.si, miha.strehar@um.si

Prispevek obravnava porast bančnih prevar, pri katerih napadalci namesto iskanja tehničnih ranljivosti uporabljajo napreden socialni inženiring (telefonske klice) in legitimna orodja za oddaljeni dostop (npr. AnyDesk). Čeprav močna avtentikacija (SCA) znižuje splošno tveganje, so trenutni pristopi v elektronskem bančništvu ranljivi, saj vse varnostne faktorje združujejo na eni kompromitirani napravi. Vrzel lahko premostijo napredne tehnologije, kot je standard v pripravi Secure Payment Confirmation (SPC). Banke trenutno odgovornost pogosto prelagajo na žrtve zaradi »hude malomarnosti«. Novejša sodna praksa in izkušnje alternativnega reševanja sporov (IRPS) potrjujejo, da podleganje manipulaciji ne sme samodejno pomeniti hude malomarnosti. Prihajajoča evropska zakonodaja (PSR in PSD3) bo to izrecno prepovedala in ob uspešnem lažnem predstavljanju uvedla jasnejšo odgovornost bank ter pogoje povračila sredstev. Poudarek kibernetske varnosti se tako premika od preverjanja identitete (»kdo si«) k potrjevanju dejanskega razumevanja in namena transakcije.

Ključne besede:
bančne prevare
socialni inženiring
močna avtentikacija
huda malomarnost
plačilni predpisi

Univerzitetna založba Univerze v Mariboru

ISBN 978-961-299-188-3
DOI https://doi.org/10.18690/um.feri.7.2026.1

1 Uvod

Digitalizacija finančnih storitev in implementacija revidirane direktive o plačilnih storitvah (PSD2) sta v evropskem prostoru bistveno spremenili varnostne zahteve elektronskega bančništva. Z obvezno uvedbo močne avtentikacije strank (angl. »Strong Customer Authentication« - SCA) naj bi se zmanjšalo število klasičnih prevar, ki so temeljile na preprosti kraji identitete ali prestrezanju statičnih gesel. Vendar kibernetski prostor ostaja dinamičen ekosistem, v katerem se napadalci hitro prilagajajo novim regulativnim zahtevam. Namesto neposrednih tehničnih vdorov v bančne sisteme so napadalci težišče svojih napadov preusmerili na najšibkejši člen kibernetske varnosti - človeka.

Skupno poročilo Evropskega bančnega organa (EBA) in Evropske centralne banke (ECB) o plačilnih prevarah izpostavlja zaskrbljujoč trend. Čeprav močna avtentikacija znižuje splošno stopnjo tveganja, se je preostalo tveganje izrazito zgostilo znotraj transakcij, ki so uspešno avtenticirane z mehanizmi SCA. Danes več kot polovico vrednosti vseh kreditnih prenosov v Evropskem gospodarskem prostoru (EGP), ki temeljijo na goljufiji, predstavljajo prevare vrste »odobreno potisno plačilo« (angl. »Authorised Push Payment« - APP), pri katerih je plačnik s pomočjo socialnega inženiringa zmanipuliran do te mere, da sam z uporabo vseh zahtevanih varnostnih elementov odobri sporno transakcijo. [1]

Izhodišče te raziskave je specifičen, forenzično obravnavan in vse pogostejši tip incidenta, pri katerem storilec z uporabo naprednega socialnega inženiringa, najpogosteje v obliki telefonskega klica (angl. »vishing«) in popolnoma legitimnih aplikacij za oddaljeni dostop (angl. »Remote Access Tools« - RAT), kot sta AnyDesk in TeamViewer, prevzame nadzor nad uporabnikovo napravo. Z namenom iskanja sistemskih rešitev za izoliranje najšibkejšega člena kibernetske varnosti se ta prispevek osredotoča na identifikacijo in analizo tehnološke vrzeli na področju arhitekture avtentikacijskih mehanizmov. Primerja najsodobnejše (angl. »state-of-the-art« - SOTA) pristope k potrjevanju transakcij, kot so kriptografski ključi (angl. »passkeys«) in specifikacija za varno potrjevanje plačil, ki je še v pripravi (angl. »Secure Payment Confirmation« - SPC), z dejansko razširjenimi, a pogosto nezadostnimi praksami, ki jih trenutno uporablja bančna industrija v EU.

Vzporedno s tehnološko analizo prispevek obravnava pravni in regulatorni vidik tovrstnih dogodkov. Jedro pravnih sporov ob zlorabah elektronskih bank namreč predstavljata opredelitev in dokazovanje »hude malomarnosti« (»gross negligence«) na strani uporabnika. Analiza vključuje slovenski zakonodajni okvir, usmeritve in opozorila nacionalnih organov ter organizacij (SI-CERT, Urad Vlade RS za informacijsko varnost - URSIV, Združenje bank Slovenije - ZBS, Varni na internetu), prakse alternativnega reševanja sporov pri ZBS ter sodno prakso in prihajajoča evropska direktiva (PSD3) in uredba (PSR), ki bosta temeljito prenovili opredelitev izhodišč za določanje stopnje zadostne skrbnosti in odgovornosti ponudnikov plačilnih storitev.

2 Forenzična anatomija bančne goljufije z oddaljenim dostopom

Za razumevanje omejitev trenutnih avtentikacijskih mehanizmov bomo razčlenili potek sodobnega napada, ki združuje elemente psihološke manipulacije in zlorabe tehnologije. Forenzične preiskave incidentov, obravnavanih v digitalnih laboratorijih in prijavljenih nacionalnemu odzivnemu centru SI-CERT, razkrivajo visoko strukturiran način dela napadalcev. Ti napadi ne temeljijo na iskanju ranljivosti vrste »ničelnega dne« (angl. »zero-day«) v bančni aplikaciji, temveč na t. i. taktiki »živeti od zemlje« (angl. »Living off the Land« - LotL), kjer napadalci zlorabljajo obstoječa, legitimna sistemska orodja in procese.

2.1. Faze napada in socialni inženiring

Napad se običajno odvija v več skrbno načrtovanih fazah, ki so zasnovane za postopno grajenje zaupanja in ustvarjanje občutka nujnosti:

1. Pri pripravi in vzpostavitvi prvega stika napadalci najprej pridobijo osnovne kontaktne podatke žrtev, pogosto iz javno dostopnih virov ali predhodnih vdorov v baze podatkov. Žrtev prejme navidezno legitimno sporočilo SMS ali elektronsko pošto, ki obvešča o izrednem dogodku, na primer »varnostni posodobitvi zaradi združevanja bank«, »blokadi računa zaradi sumljive aktivnosti« ali »odprtem kreditnem zahtevku«. Sporočilo vsebuje povezavo do prepričljive lažne spletne strani, kjer žrtev vnese svoje osnovne prijavne podatke in telefonsko številko.
2. Sledita lažno predstavljanje in glasovna manipulacija v obliki telefonskega klica. Klicatelji komunicirajo v tekočem slovenskem jeziku, izkazujejo visoko raven profesionalnosti in se pogosto predstavijo kot uslužbenci tehnične pomoči banke, operaterji SI-CERT-a ali celo kot predstavniki policije in Banke Slovenije. Z uporabo tehnologije potvarjanja klicne številke se lahko na zaslonu žrtve celo prikaže dejanska telefonska številka banke, kar močno poveča verodostojnost klica.
3. Pod pretvezo, da mora žrtev zaradi varnosti nujno nadgraditi sistemsko zaščito ali preveriti stanje na računu, jo klicatelj usmerja, naj iz uradne trgovine z aplikacijami (Google Play, Apple App Store) ali prek spletne strani prenese aplikacijo za oddaljeni dostop (AnyDesk, TeamViewer, Chrome Remote Desktop). Ker gre za legitimna komercialna orodja, namenjena tehnični podpori, varnostni mehanizmi operacijskega sistema in nameščeni protivirusni programi teh aplikacij ne prepoznajo kot zlonamerno programsko opremo (angl. »malware«).

2.2. Forenzični artefakti in izkoriščanje seje

Ko žrtev namesti aplikacijo in napadalcu posreduje kodo za vzpostavitev seje, napadalec pridobi popoln ali delni nadzor nad napravo. Z vidika digitalne forenzike je to ključni trenutek. Forenzične analize pomnilnika, registrov (v okolju Windows) ali datotečnega sistema Android (prenesene datoteke, medpomnilnik, dnevniške datoteke aplikacije AnyDesk) sicer jasno pokažejo, da je bila oddaljena seja vzpostavljena, da so bile prenesene datoteke ali da so se izvajali kliki. Vendar pa ti artefakti zgolj potrjujejo prisotnost oddaljene seje, pa ne omogočajo preprečevanja zlorabe, saj potekajo znotraj avtoriziranega kanala.

Napadalec na tej točki izkoristi specifične funkcionalnosti orodij za oddaljeni dostop: [2]

1. Da bi preprečil, da bi žrtev videla, kaj se dogaja na zaslonu, napadalec aktivira funkcijo zatemnitve zaslona, ki jo omogočajo orodja, kot je AnyDesk za »zasebnost« med oddaljenim delom.
2. Medtem ko je zaslon črn, napadalec na napravi žrtve odpre mobilno banko ali pa žrtev prosi, naj mu »za preverjanje« prebere kodo SMS, ki jo je pravkar prejela. Če mobilna banka uporablja potisna (angl. »push«) sporočila za avtorizacijo (npr. potrditev z vnosom varnostne PIN kode znotraj aplikacije), lahko napadalec, če je pridobil ustrezna pooblastila (npr. z uporabo storitev za dostopnost v sistemu Android), potrdi transakcijo kar sam ali pa preprosto prosi žrtev, naj na slepo ali pod lažno pretvezo potrdi postopek.
3. Sredstva se nato prenesejo na račune t. i. denarnih mul, pogosto v tujino, ali v kriptomenjalnice, kjer se sled za denarjem hitro izgubi.

3 Omejitve obstoječih sistemov avtentikacije

Iz opisane anatomije napada sledi arhitekturna napaka v načinu, kako bančne institucije v EU in Sloveniji implementirajo zahteve direktive PSD2 v delu, ki se nanaša na močno avtentikacijo strank. [3][4] Predpisi od ponudnikov plačilnih storitev zahtevajo preverjanje na podlagi dveh od treh neodvisnih elementov (nekaj, kar vem, nekaj, kar imam, nekaj, kar sem). Kljub temu se v praksi soočamo z resnimi omejitvami.

3.1. Močna avtentikacija pri napadenem komitentu

Evropski bančni organ (EBA) opozarja, da čeprav se je število prevar z ukradenimi poverilnicami (angl. »unauthorised fraud«) zmanjšalo, je stopnja uspešnosti prevar pri transakcijah, ki so bile podvržene močni avtentikaciji (SCA), presenetljivo visoka. [5] Metodologija SCA, kot se trenutno izvaja v praksi (npr. SMS OTP ali preprost pritisk na gumb »Potrdi« v mobilnem žetonu ob uporabi prstnega odtisa), ne upošteva kognitivnega stanja uporabnika. Če je bil uporabnik žrtev socialnega inženiringa in je prepričan, da s potrditvijo transakcije dejansko »odpravlja blokado računa«, bo brez oklevanja zagotovil zahtevana faktorja (telefon in prstni odtis).

V takšnem primeru SCA ne deluje več kot varnostna pregrada pred prevaro, temveč postane izjemno zanesljivo forenzično in kriptografsko orodje za potrditev napačne odločitve. Napadi z dajanjem navodil po telefonu in z uporabo orodij za oddaljeni dostop (RAT) uspejo prav zato, ker obidejo tehnične kontrole in izkoristijo uporabnikovo napačno razumevanje konteksta.

3.2. Tveganje zgostitve vseh faktorjev na eni napravi

Največja praktična in arhitekturna slabost sodobnega elektronskega bančništva je zgostitev (koncentracija) vseh avtentikacijskih faktorjev in odločevalskih procesov na eni sami končni napravi (npr. pametnem telefonu). Koncept večfaktorske avtentikacije zgodovinsko temelji na predpostavki ločenih in neodvisnih kanalov (angl. »Out-of-Band« - OOB). Če napadalec kompromitira računalnik, nima dostopa do pametne kartice v žepu uporabnika ali do njegovega ločenega telefona.

V sodobnem mobilnem bančništvu pa uporabnik na isti napravi:

1. Posluša navodila napadalca (telefonski klic).
2. Upravlja vmesnik spletne ali mobilne banke.
3. Prejema drugi varnostni faktor (SMS žeton ali potisno potrditev v ločeni aplikaciji).
4. Dovoljuje izvajanje aplikacije za oddaljeni dostop, ki zajema zaslon.

S tem se odpira vprašanje dejanske neodvisnosti faktorjev, ki ga zahteva 9. člen Regulativnih tehničnih standardov (RTS) za SCA (Uredba EU 2018/389). Z oddaljenim dostopom se vzpostavi enotno kompromitirano okolje. Prevarant z dostopom do zaslona (ali na primer z uporabo storitev za dostopnost za branje vsebine na sistemu Android) lahko v realnem času prestereže kodo OTP iz SMS sporočila in jo vnese v plačilni nalog, ne da bi uporabnik, katerega zaslon je zatemnjen, to opazil. Zanašanje industrije izključno na posest naprave in biometrično odklepanje zaslona postane neučinkovito, če naprava ni pod popolnim nadzorom uporabnika.

4 Napredne metode potrjevanja

Da bi presegli omejitve trenutnih praks in uspešno zajezili goljufije z oddaljenim dostopom, tehnološki konzorciji (W3C, FIDO Alliance) in napredni deležniki v plačilni industriji razvijajo in uvajajo nove asimetrične kriptografske metode avtentikacije. Te metode rešujejo problem napadov z ribarjenjem in manipulacije na strukturni ravni.

4.1. FIDO2, WebAuthn in Passkeys

Sodobna zaščita identitete (SOTA) opušča statična gesla in SMS potrditve ter prehaja na arhitekturo FIDO2 (angl. »Fast IDentity Online«) in standard WebAuthn, bolj znan pod komercialnim imenom »passkeys« (kriptografski ključi). [6]

Namesto da bi si uporabnik in banka delila »skrivnost« (geslo ali kodo), passkeys temeljijo na asimetrični kriptografiji javnega in zasebnega ključa. Zasebni ključ se generira in trajno hrani izključno v varni strojni enklavi naprave (angl. »Secure Enclave« ali »Trusted Platform Module« - TPM) in v različici passkeys, ki je vezana na napravo, naprave nikoli ne zapusti.

Avtentikacija se izvede lokalno: banka (angl. »relying party«) pošlje kriptografski izziv (angl. »challenge«), naprava pa preveri identiteto uporabnika (z biometrijo ali kodo PIN) in izziv podpiše z zasebnim ključem. Ker je kriptografski podpis neločljivo vezan na specifično spletno domeno (angl. »origin-bound«), je ta metoda že po zasnovi odporna proti klasičnim napadom z ribarjenjem. Tudi če uporabnik podatke vpisuje na lažni strani (npr. lažnabanka.si), se kriptografski podpis, ustvarjen za to domeno, ne bo ujemal z javnim ključem na strežniku prave banke.

Omejitve tehnologije passkeys v zvezi z direktivo PSD2 so povezane s tem, da čeprav so passkeys učinkoviti za prijavo v sistem, v svoji osnovni obliki protokola WebAuthn (metoda webauthn.get) ne zadoščajo za izpolnjevanje specifičnih zahtev PSD2 glede potrjevanja plačil. PSD2 (v 5. členu RTS) namreč zahteva dinamično povezovanje (angl. »Dynamic Linking«). To pomeni, da mora biti avtentikacijska koda neločljivo specifična za natančen znesek transakcije in identiteto prejemnika. Kakršna koli poznejša sprememba zneska ali prejemnika mora povzročiti neveljavnost avtentikacijske kode. Poleg tega mora biti zagotovljeno zavedanje plačnika (angl. »Payer Awareness«) - uporabniku morata biti pred potrditvijo nedvoumno prikazana znesek in prejemnik. Navaden izziv WebAuthn je zgolj naključno generiran niz podatkov brez semantičnih informacij o transakciji, zato sama prijava v sistem s tehnologijo passkey ne ustreza določilom o dinamičnem povezovanju.

4.2. Standard Secure Payment Confirmation (SPC) kot rešitev tehnološke vrzeli

Za premostitev te vrzeli je konzorcij W3C (angl. »World Wide Web Consortium«) v sodelovanju z zavezništvom FIDO in plačilno industrijo razvil specializirani standard spletnega vmesnika API za varno potrjevanje plačil (angl. »Secure Payment Confirmation« - SPC). [7] Ta gradi neposredno na infrastrukturi WebAuthn in ji dodaja ključne plačilne mehanizme, ki omogočajo popolno skladnost z zahtevami PSD2 in prihajajoče direktive PSD3.

Mehanizem SPC vzpostavlja model »kar vidiš, to podpišeš« (angl. »What-you-see-is-what-you-sign«) z naslednjimi tehnološkimi značilnostmi:

1. Vgrajeni prikaz v brskalniku (angl. »Browser-native UI«). Kadar banka zahteva potrditev plačila z uporabo SPC, API v uporabnikovem brskalniku (ali operacijskem sistemu) sproži prikaz posebnega, standardiziranega pogovornega okna (dialoga). To okno nadzoruje operacijski sistem in ne spletna stran, zato ga zlonamerna skripta ali prevarant z osnovnim zajemom zaslona bistveno težje prikrije ali ponaredi. V tem oknu so neločljivo prikazani točen znesek, valuta in ime prejemnika (angl. »merchant/payee«).
2. Najpomembnejša inovacija SPC je kriptografska povezava transakcijskih podatkov z neposredno vključitvijo prikazanih konkretnih plačilnih podatkov v podatkovno strukturo, ki je podpisana. Tako sta znesek in podatki o prejemniku vključena v podatke, ki jih SPC prikaže uporabniku.
3. Ker so transakcijski podatki kriptografsko zapečateni in vgrajeni v sam avtentikacijski zahtevek neposredno z uporabo strojne enklave, napadalec ne more naknadno spremeniti podatkov o nakazilu, ne da bi s tem razveljavil veljavnost ustvarjene potrditvene kode.

Kot izhaja iz primerjave v tabeli 1, bi implementacija arhitekture SPC namesto enostavnih enkratnih gesel SMS ali generičnih mobilnih žetonov predstavljala pomemben napredek na področju varnosti. Kljub temu tehnološka vrzel ostaja velika, saj banke zaradi stroškov integracije, skrbi glede uporabniške izkušnje in počasnega sprejemanja standardov v vseh brskalnikih še vedno vztrajajo pri zastarelih in ranljivih metodah. S tem tveganje oddaljenega prevzema naprave nesorazmerno prenašajo na komitente.

Tabela 1: Primerjava varnosti metod potrjevanja plačil

Merilo varnosti (PSD2/PSD3 zahteve)	SMS OTP (praksa v postopnem opuščanju)	Potisna avtentikacija	W3C Secure Payment Confirmation (SOTA)
Prikaz zavedanja plačnika (angl. »Payer Awareness«)	Znotraj besedila SMS sporočila (pogosto ignorirano).	Ločena aplikacija (pogosto le obvestilo »Potrdite transakcijo«).	**Vgrajeni dialog operacijskega sistema**, specifičen za plačilo, nadzorovan zunaj vpliva spletne strani.
Odpornost na ribarjenje (prestrezanje poverilnic)	Nizka. Uporabnik prebere in vnese kodo na lažni strani.	Srednja. Zanaša se na to, da uporabnik preveri podrobnosti.	**Odporna.** Kriptografija je neločljivo povezana s pravo domeno banke (angl. »origin-bound«).
Dinamično povezovanje (angl. »Dynamic Linking«)	Koda je povezana z zneskom na zalednem sistemu banke.	Koda je poslana v aplikacijo, znesek je prikazan v uporabniškem vmesniku.	**Kriptografsko vgrajeno.** Znesek in prejemnik sta del objekta CollectedClientData, podprtega s strojnim ključem.
Odpornost proti zlorabi z AnyDesk/RAT	**Ranljiv.** Napadalec prebere SMS na zatemnjenem zaslonu ali ga razkrije žrtev sama.	**Nizka odpornost.** Napadalec lahko sam klikne gumb »potrdi« ali usmerja žrtev.	**Visoka odpornost.** Zahteva eksplicitno lokalno potrditev točnega zneska na ravni operacijskega sistema, ki ga RAT težje manipulira brez prekinitve podpisa.

4.3. Preverjanje prejemnika (Verification of Payee - VoP) kot komplementarni zaščitni sloj

Kadar tehnološke ovire same po sebi ne morejo preprečiti, da bi zavedeni uporabnik izvedel avtentikacijo transakcije, je nujno uvesti kontrolne mehanizme, ki prekinejo kognitivno zanko napadalca in ustvarijo t. i. pozitivno trenje (angl. »friction«) pred končnim odlivom sredstev. Forenzična analiza primerov zlorab z oddaljenim dostopom in telefonskim klicem (RAT/vishing) kaže, da ena ključnih točk prevare nastopi, ko storilec žrtvi narekuje vnos tuje številke IBAN (račun denarne mule) in ji zagotovi, da gre za »varen račun«, »rezervni račun pri Banki Slovenije« ali »FURS«. Žrtev pod vplivom stresa ne preverja lastništva računa, saj do nedavnega to v sistemu SEPA ni bilo niti tehnološko mogoče v realnem času.

Kot ključen varnostni ukrep in rešitev tega problema je Evropska unija v okviru Uredbe o takojšnjih plačilih in prihajajoče Uredbe o plačilnih storitvah (PSR) uzakonila storitev Preverjanje prejemnika (angl. »Verification of Payee – VoP«). [8] VoP vzpostavlja obveznost bank, da plačniku še pred potrditvijo in izvršitvijo kreditnega prenosa omogočijo preverjanje ujemanja med vnesenim imenom prejemnika in dejanskim imenom imetnika ciljnega računa IBAN. Ta mehanizem je postal obvezen in brezplačen za kreditne prenose v eurih v evroobmočju 9. oktobra 2025, nova uredba PSR pa ga širi na vse valute znotraj EU.

V scenariju, kjer napadalec z uporabo orodja za oddaljeni dostop (npr. AnyDesk) prevzame nadzor in vnese račun IBAN denarne mule, medtem ko žrtvi zatrjuje, da gre za »pokojninski sklad«, sistem VoP pred zahtevo po biometrični potrditvi vrne opozorilo o neujemanju ali prikaz dejanskega imena lastnika računa. Takšno eksplicitno in v realnem času generirano opozorilo v številnih primerih zadostuje, da posvari žrtev v stanju psihološke manipulacije in zmanjša uspešnost socialnega inženiringa na primer pri direktorskih prevarah in prevar vmešavanja v komunikacijo (angl. »Business Email Compromise« - BEC), vendar je brez učinka, kadar lahko napadalec z oddaljenim dostopom popolnoma samostojno in brez sodelovanja žrtve ustvari in potrdi plačilni nalog s podatki poljubnega prejemnika.

5 Pravni okvir in doktrina hude malomarnosti v slovenskem in evropskem pravu

Presečišče kompleksnih informacijskih tehnologij in prava pride do polnega izraza v trenutku po izvršeni zlorabi, ko komitent (potrošnik) od svoje banke zahteva vračilo odtujenih sredstev. Pravni spori, povezani z zlorabami elektronskega bančništva z uporabo socialnega inženiringa, se primarno osredotočajo na porazdelitev odgovornosti in razlago pravnih standardov skrbnosti.

5.1. ZPlaSSIED in odgovornost ponudnika

V slovenskem pravnem redu je področje izvajanja plačilnih storitev in odgovornosti zanje urejeno v Zakonu o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED), s katerim je bila direktiva PSD2 prenesena v nacionalno zakonodajo. [9]

Zakon izhaja iz temeljnega načela zaščite potrošnika. V primeru neodobrene plačilne transakcije je v skladu s 136. členom ZPlaSSIED ponudnik plačilnih storitev (banka) dolžan plačniku nemudoma oziroma najpozneje do konca naslednjega delovnega dne, povrniti znesek te transakcije. V digitalnem forenzičnem laboratoriju opažamo, da se banke pogosto sklicujejo na izjemo, predpisano v 137. členu ZPlaSSIED. Ta člen določa odstopanje od obveznosti vračila in prenos celotnega bremena izgube na uporabnika, če je do izvršitve neodobrene plačilne transakcije prišlo zaradi uporabnikovega naklepa ali zato, ker je uporabnik iz hude malomarnosti (angl. »gross negligence«) kršil svoje obveznosti glede varovanja osebnih varnostnih elementov, določene v 132. členu istega zakona.

5.2. Pravni standard hude malomarnosti in splošni pogoji bank

Pojem »huda malomarnost« v ZPlaSSIED ni izrecno opredeljen, temveč gre za t. i. nedoločen pravni pojem ali pravni standard, katerega vsebino morajo v vsakem posamičnem primeru napolniti sodišča na podlagi konkretnih okoliščin.

V sodni praksi velja, da je huda malomarnost podana takrat, ko oseba ravna skrajno nepazljivo in znatno odstopa od skrbnosti, ki se v posameznem primeru lahko pričakuje od povprečno skrbnega človeka, kar nakazuje na zavestno zanemarjanje običajnih varnostnih ukrepov.

Da bi zmanjšale svojo izpostavljenost tveganjem, banke ta nedoločen pravni pojem pogosto enostransko opredeljujejo v svojih splošnih pogojih poslovanja (SPP). V teh pogojih so kot huda malomarnost rutinsko našteta dejanja, kot so:

- Posredovanje uporabniškega imena, gesla ali potrditvene kode SMS kateri koli tretji osebi ali njihov vnos na nepreverjeno spletno stran.
- Neuporaba posodobljenih licenčnih protivirusnih programov na napravi.
- Omogočanje oddaljenega dostopa do naprave (z uporabo programov RAT, kot je AnyDesk) na zahtevo neznanih oseb.

Zveza potrošnikov Slovenije (ZPS) in Evropska potrošniška organizacija (BEUC) ostro opozarjata na nevzdržnost prakse, pri kateri si banke prisvajajo pravico, da same določajo meje hude malomarnosti. Po prepričanju teh organizacij banke s samodejnim pripisovanjem hude malomarnosti ob uspešnem ribarjenju izkrivljajo bistvo direktive PSD2 in prelagajo celotno odgovornost (in s tem tudi tveganje zaradi lastnih tehnoloških vrzeli v avtentikaciji) izključno na potrošnika. BEUC poudarja, da gola dejstva (npr. da so bili vneseni vsi varnostni elementi) ne bi smela veljati za neizpodbiten dokaz hude malomarnosti in da mora dokazno breme nedvoumno ostati na strani banke. [14]

5.3. Slovenska in evropska sodna praksa

V slovenski sodni praksi obstajajo pomembne odločitve višjih sodišč in vrhovnega sodišča (npr. VSL I Cpg 160/2025 z dne 17. 9. 2025, VSL Sodba I Cpg 82/2019, VSL Sodba II Cp 1212/2022, VSL Sklep I Cpg 76/2024), ki presojajo vprašanje malomarnosti.

Sodišča so v nekaterih primerih pritrdila bankam in presodila, da popolna odsotnost kritične presoje, na primer posredovanje varnostnih podatkov na očitno lažni spletni strani in zamolčanje te okoliščine banki ob prijavi incidenta, izpolnjuje standard hude malomarnosti. Kljub temu pa je presoja v primerih dobro načrtovanega in izvedenega telefonskega klica ter zlorabe z AnyDeskom bolj zapletena.

Ob upoštevanju psihološkega stresa, ki ga povzroči avtoritativni klic »policista« ali »bančnika«, ki žrtvi grozi z izgubo življenjskih prihrankov, je mnogim potrošnikom zelo težko očitati zavestno zanemarjanje skrbnosti. Takšno ravnanje pogosto ustreza navadni (lahki) malomarnosti, pri kateri pa finančno breme nosi banka. V širšem evropskem prostoru se vzpostavlja strožja doktrina odgovornosti ponudnikov plačilnih storitev. Sodišče Evropske unije (CJEU) v zadevah, kot je C-70/25 (Tukowiecka), ki je še v teku, obravnava vprašanje takojšnjega vračila sredstev. [10] Trenutno pravno razumevanje (ki so ga med drugim potrdila španska, francoska in italijanska vrhovna sodišča) poudarja, da zgolj elektronski zapis v informacijskem sistemu banke, ki potrjuje, da je bila transakcija uspešno avtenticirana z močnimi varnostnimi elementi, še ne zadostuje kot dokaz, da je transakcijo avtoriziral uporabnik, niti ne zadostuje za dokazovanje hude malomarnosti. Sodišča (npr. v Nemčiji) v številnih primerih razsojajo, da to, da se žrtev ujame v past socialnega inženiringa (kljub vnosu podatkov) ne predstavlja hude malomarnosti, zaradi česar morajo banke prevzeti finančno odgovornost za škodo. Prav tako primeri iz Avstrije (npr. OLG Linz) opozarjajo na odgovornost banke. Tudi če je bil potrošnik malomaren, sodišča presojajo soodgovornost banke, kadar njen sistem za spremljanje prevar (angl. »Fraud Transaction Monitoring« - FTM) ni pravočasno prepoznal in blokiral očitno nenavadnih serijskih transakcij takoj po namestitvi nove aplikacije (deljena odgovornost 50:50). [11]

5.4. Izkušnje iz alternativnega reševanja sporov pri Združenju bank Slovenije (IRPS)

Kadar potrošnik in banka ne dosežeta sporazuma v internem pritožbenem postopku glede odgovornosti za spletno zlorabo, imajo komitenti možnost sprožiti postopek pri izvajalcu izvensodnega reševanja potrošniških sporov (IRPS), ki deluje v okviru Združenja bank Slovenije (ZBS).

Poročila o delovanju IRPS za leti 2023 in 2024 kažejo, da so spori, ki izvirajo iz spletnih in mobilnih prevar (ribarjenje, investicijske prevare z zlorabo oddaljenega dostopa), med najpogostejšimi zadevami. Leta 2023 je IRPS obravnaval in zaključil 130 zadev. Leta 2024 je IRPS posebej zabeležil porast novih tipov zlorab, pri katerih so uporabniki s prenosom zlonamerne kode ali aplikacij omogočili goljufom oddaljen dostop do naprav in s tem do mobilne banke [12][13]. ZBS na svojem portalu »Varni na internetu« in v svojih smernicah redno opozarja na te grožnje in komitentom predpisuje obsežen seznam deloma tudi zahtevnih varnostnih priporočil.

Čeprav je postopek za potrošnika brezplačen in naj bi omogočal hitro rešitev spora, je njegova ključna pomanjkljivost v dejstvu, da so izdana mnenja posrednika v sporu za banke nezavezujoča.

Tudi v primerih, ko posrednik IRPS po pregledu dejstev ugotovi, da potrošnik, ki je bil žrtev naprednega ribarjenja, ni ravnal s hudo malomarnostjo in izda mnenje v njegovo korist, se številne banke odločijo, da tega mnenja preprosto ne upoštevajo in odklonijo povračilo sredstev. V javnosti je odmeval primer potrošnika, ki je v nočnem

času kupoval prek spleta (Amazon) in je bil tarča zlorabe. Iz njegovega računa je bilo v Estonijo prenakazanih skoraj 8.000 EUR. Potrošnik je imel ustrezno zaščito računalnika. Čeprav mu je poravnalni svet ZBS pritrdil in podal mnenje v njegovo korist, je banka povračilo vztrajno zavračala, kar je potrošnika prisililo k vložitvi drage in tvegane tožbe na sodišču. Takšna praksa nakazuje, da alternativno reševanje sporov brez zavezujočih odločitev v trenutnem pravnem vakuumu razlage hude malomarnosti ne zagotavlja ustreznega varstva potrošnikov pred naraščajočimi kibernetskimi tveganji. Kljub vsemu pa podatek, da so banke v letu 2024 pri IRPS sklenile sporazume ali poravnave v približno 27 odstotkih obravnavanih zadev (37 primerov), kaže na to, da se tudi znotraj bančne industrije postopoma krepi zavedanje o nesmiselnosti prelaganja absolutne odgovornosti na manipulirane žrtve, zlasti ob potencialnih pomanjkljivostih lastnih opozorilnih sistemov.

5.5. Prihajajoča regulativna paradigma: Uredba o plačilnih storitvah (PSR) in PSD3

Zaradi nezadostnosti trenutnega okvira PSD2 v boju proti prevaram in zlorabam socialnega inženiringa je Evropska komisija pripravila predloga tretje direktive o plačilnih storitvah (PSD3) in uredbe o plačilnih storitvah (PSR). Ker bo PSR sprejeta v obliki uredbe, se bo neposredno in enotno uporabljala v vseh državah članicah, s čimer bo odpravljeno trenutno razdrobljeno nacionalno razumevanje varnosti in odgovornosti. [15][16]

Nova zakonodaja prinaša prelomne premike:

1. PSR uvaja jasnejšo odgovornost bank za primere, ko goljuf, ki se izdaja za uslužbenca banke, zavede potrošnika. Tudi če je uporabnik transakcijo tehnično avtoriziral (pod vplivom telefonskega klica in oddaljenega dostopa), mora banka v primeru pravočasne prijave incidenta ter podane prijave policiji uporabniku povrniti celoten znesek izgube. S tem se odgovornost za sistemsko preprečevanje prevar izrecno prenaša nazaj na ponudnike infrastrukture.
2. Banke bodo še vedno imele možnost zavrniti povračilo v primerih potrošnikove »hude malomarnosti«, vendar bo prag dokazovanja znatno višji. Samo dejstvo, da je potrošnik pod vplivom naprednega socialnega inženiringa nasedel prevari, zakonsko ne bo več obravnavano kot huda malomarnost. Banke bodo morale izvesti temeljito preiskavo in predložiti neizpodbitne dokaze o grobem kršenju pravil.
3. PSR prepoznava dejstvo, da se socialni inženiring in deljenje zlonamernih povezav najpogosteje ne zgodita znotraj same bančne aplikacije, temveč na telekomunikacijskih omrežjih, družbenih omrežjih (Facebook, TikTok) in iskalnikih. Nova ureditev omogoča bankam, da pod določenimi pogoji regresirajo (zahtevajo povračilo) od velikih spletnih in telekomunikacijskih družb, če so te z neukrepanjem po prijavi ali z neustreznim nadzorom (npr. omogočanjem lažnega prikazovanja klicnih številk) dopustila izvedbo prevare.
4. Banke bodo morale obvezno uvesti in nadgraditi mehanizme za spremljanje tveganj, predvsem pa bodo upravičene in zakonsko obvezane blokirati in zadržati zelo tvegana nakazila v realnem času, za kar bodo lahko prosto izmenjevale indikatorje zlorab z drugimi ponudniki (angl. »shared fraud data«).

6 Sklep

Sodobne prevare z uporabo aplikacij za oddaljeni dostop in naprednega socialnega inženiringa izpodbijajo klasične predpostavke kibernetske varnosti v elektronskem bančništvu. Dokler bodo finančne institucije zahteve po dveh avtentikacijskih faktorjih združevale na eni sami končni napravi z uporabo generičnih potisnih sporočil in tehnologij SMS, bo oddaljena zloraba te naprave uspešno zaobšla celoten varovalni obroč. Identificirana tehnološka vrzel nakazuje, da so v pripravi izboljšave v obliki standarda W3C Secure Payment Confirmation (SPC), ki temelji na biometričnem in kriptografskem potrjevanju na ravni strojne enklave, pri čemer na zaslonu operacijskega sistema nespremenljivo in nezamenljivo prikaže dejanski znesek in prejemnika nakazila. Izgovori za vztrajanje pri zastareli avtentikaciji ob pojavu takšnih naprednih standardov niso več strokovno vzdržni. Rutinsko prelaganje celotne finančne odgovornosti na uporabnike pod izgovorom hude malomarnosti samo zato, ker so

pod hudim psihološkim pritiskom »lažnega uslužbenca« posredovali podatke ali namestili legitimno programsko opremo, lahko predstavlja izkrivljanje stanja. Forenzična analiza in izkušnje IRPS ter tuja sodišča kažejo, da zgolj zavajanje potrošnika v napredni prevari ne sme dosegati praga hude malomarnosti, dokazno breme pa mora ostati na banki. Nova pravila Uredbe o plačilnih storitvah (PSR) bodo to usmeritev uzakonila z uvedbo obveznega povračila sredstev pri poosebljanju bank. Izključno tehnično preverjanje identitete ni dovolj. Varnostni sistemi morajo preverjati namen in kontekst transakcije. Uvedba storitve Verification of Payee (VoP) bo z obveznim opozarjanjem na neujemanje med imenom in številko IBAN prejemnika predstavljala pomemben dodatni element kognitivnega trenja, ki ga napadalci ob uporabi oddaljenega dostopa ne bodo imeli možnosti zlahka prikriti s prepričljivo zgodbo. Varovanje sredstev komitentov se premika od preverjanja »ali ste to res vi« k preverjanju »ali zares veste in razumete, komu in zakaj nakazujete sredstva«. Šele praksa pa bo pokazala, ali se bodo uporabniki elektronskega bančništva pustili pretentati tako, da bodo na podlagi navodil napadalca sami potrjevali sumljive transakcije. Za slabo presojo pa trenutno nimamo tehnične rešitve.

Literatura

[1] European Banking Authority, European Central Bank: 2025 Report on Payment Fraud, EBA/REP/2025/40, december 2025, https://www.eba.europa.eu/sites/default/files/2025-12/1709846a-84d9-47cf-86a0-b155efb34d66/EBA%20and%20ECB%20Report%20on%20Payment%20Fraud.pdf, obiskano 3. 7. 2026.

[2] SI-CERT: Napredni phishing napadi na spletne banke podjetij z elementom telefonskega klica, 29. 10. 2025, https://www.cert.si/napredni-phishing-napadi-na-spletne-banke-podjetij-z-elementom-telefonskega-klica/, obiskano 3. 7. 2026.

[3] Direktiva (EU) 2015/2366 z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES in 2013/36/EU ter Uredbe (EU) št. 1093/2010 in razveljavitvi Direktive 2007/64/ES, Uradni list Evropske unije, L 337, 23. 12. 2015, str. 35–127, https://eur-lex.europa.eu/eli/dir/2015/2366/oj, obiskano 5. 7. 2026.

[4] Delegirana uredba Komisije (EU) 2018/389 z dne 27. novembra 2017 o dopolnitvi Direktive (EU) 2015/2366 glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupne in varne odprte standarde komunikacije, Uradni list Evropske unije, L 69, 13. 3. 2018, str. 23–43, https://eur-lex.europa.eu/eli/reg_del/2018/389/oj, obiskano 5. 7. 2026.

[5] https://www.zbs-giz.si/oblike-prevar-njihovi-znaki-in-opisi-ter-priporocljiva-ravnanja-bank, Združenje bank Slovenije: Oblike prevar, njihovi znaki in opisi, obiskano 23. 7. 2026.

[6] W3C: Web Authentication: An API for Accessing Public Key Credentials – Level 2, W3C Recommendation, 8. 4. 2021, https://www.w3.org/TR/webauthn-2/, obiskano 7. 7. 2026.

[7] W3C: Secure Payment Confirmation, Candidate Recommendation Draft, 2. 7. 2026, https://www.w3.org/TR/secure-payment-confirmation/, obiskano 3. 8. 2026.

[8] Uredba (EU) 2024/886 z dne 13. marca 2024 o spremembi uredb (EU) št. 260/2012 in (EU) 2021/1230 ter direktiv 98/26/ES in (EU) 2015/2366 glede takojšnjih kreditnih prenosov v eurih, Uradni list Evropske unije, L 2024/886, 19. 3. 2024, https://eur-lex.europa.eu/eli/reg/2024/886/oj, obiskano 3. 8. 2026.

[9] Zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih – ZPlaSSIED, Uradni list Republike Slovenije, št. 7/18, 9/18 – popr. in 102/20, https://pisrs.si/pregledPredpisa?id=ZAKO7574, obiskano 9. 7. 2026.

[10] RANTOS Athanasios: Sklepni predlogi generalnega pravobranilca v zadevi C-70/25, Tukowiecka, z dne 5. 3. 2026, ECLI:EU:C:2026:153, Sodišče Evropske unije, https://infocuria.curia.europa.eu/tabs/jurisprudence?publishedId=C-70%2F25, obiskano 3. 7. 2026.

[11] OBERLANDESGERICHT LINZ: Odločba 1 R 45/25f z dne 22. 5. 2025, Rechtsinformationssystem des Bundes – RIS, https://www.ris.bka.gv.at/, obiskano 3. 7. 2026.

[12] Združenje bank Slovenije: Poročilo o delovanju izvajalca izvensodnega reševanja potrošniških sporov pri Združenju bank Slovenije za leto 2023, 2024, https://www.zbs-giz.si/irps/, obiskano 5. 7. 2026.

[13] Združenje bank Slovenije: Poročilo o delovanju izvajalca izvensodnega reševanja potrošniških sporov pri Združenju bank Slovenije za leto 2024, 2025, https://www.zbs-giz.si/irps/, obiskano 5. 7. 2026.

[14] The European Consumer Organisation: Payment Services: BEUC's Recommendations on the Payment Services Regulation and the Payment Services Directive 3, BEUC-X-2023-123, 29. 9. 2023, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-123_Payments_Services_Recommendations%20on%20the%20PSR-PSD3.pdf, obiskano 9. 7. 2026.

[15] Predlog direktive Evropskega parlamenta in Sveta o plačilnih storitvah in storitvah elektronskega denarja na notranjem trgu, spremembi Direktive 98/26/ES ter razveljavitvi direktiv (EU) 2015/2366 in 2009/110/ES, COM(2023) 366 final, 2023/0209(COD), 28. 6. 2023, https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:52023PC0366, obiskano 10. 7. 2026.

[16] Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market, amending Directive 98/26/EC and repealing Directives (EU) 2015/2366 and 2009/110/EC – Confirmation of the final compromise text with a view to agreement, dokument ST 8222/26, 17. 4. 2026, https://data.consilium.europa.eu/doc/document/ST-8222-2026-INIT/en/pdf, obiskano 16. 7. 2026.