Utjecaj COVID-19 pandemije na sigurnost platnog prometa i percepciju korisnika o zaštiti bezgotovinskih transakcija

Sučić, Karlo

Sveučilište u Zagrebu

Ekonomski Fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija - smjer Menadžerska informatika

Utjecaj COVID-19 pandemije na sigurnost platnog prometa i percepciju korisnika o zaštiti bezgotovinskih transakcija

Diplomski rad

Karlo Sučić

Zagreb, rujan 2021.

Sveučilište u Zagrebu

Ekonomski Fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija - smjer Menadžerska informatika

Utjecaj COVID-19 pandemije na sigurnost platnog prometa i percepciju korisnika o zaštiti bezgotovinskih transakcija

The impact of the COVID-19 pandemic on payment security and users' perception of the protection of non-cash transactions

Diplomski rad

Student: Karlo Sučić

JBMAG studenta: 0067544228

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, rujan 2021.

Sažetak

Cilj rada je na osnovu temeljitog istraživanja prikazati i identificirati sigurnosne mjere i rizike donesene u doba COVID-19 pandemije (krize) i njihov utjecaj na sigurnost platnog prometa. U radu je detaljno predstavljena identifikacija i analiza rizika, mjere sigurnosti (zaštite) i čimbenika platnog prometa te okruženje koje je utjecalo na donošenje takvih mjera. U drugom dijelu rada anketnim istraživanjem percepcije korisnika o sigurnosti bezgotovinskih transakcija dokazat će se uspješnost provedenih mjera donesenih u cilju povećanja sigurnosti bezgotovinskih transakcija krajnjih korisnika u doba pandemije, a time i cijelog platnog sustava kojeg su većinom činile bezgotovinske transakcije. Konačan cilj bit će predstavljen na kraju rada vlastitim opažanjem o sigurnosti platnog prometa na temelju provedenog istraživanja.

Ključne riječi: platni promet, bezgotovinske transakcije, COVID-19 pandemija, identifikacija rizika, sigurnost platnog prometa, sigurnosne mjere

Summary

The goal of this paper is to present and identify security measures and risks adopted during the COVID-19 pandemic (crisis) and their impact on payment security, based on basic research. The paper presents in detail the identification and analysis of risks, security measures (protection), payment factors and other environment factors that influenced the adoption of such measures. In the second part of the paper, a survey of users' perceptions of the security of non-cash transactions will prove the success of measures taken to increase the security of non-cash transactions of end users during the pandemic and the entire payment system, which mostly was consisted of non-cash transactions. The final goal will be presented at the end of the paper by own observation on payment security, based on proven research.

Key words: payment operations, non-cash transactions, COVID-19 pandemic, risk identification, payment security, security measures

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora, te da nijedan dio diplomskog rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(vlastoručni potpis)

_____

(mjesto i datum)

STATEMENT OF THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare thath no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

_____

(personal signature)

_____

(place and date)

SADRŽAJ

1. Uvod

1.1 Predmet i cilj rada

Od početka pojave banaka ljudi su stalno pokušavali naći nove načine kako učinkovito unaprijediti bankarsko poslovanje i ponuditi nešto novo svojim korisnicima te time steći konkurentsku prednost, kako bi uvijek bili jedan korak ispred svojih konkurenata. Pojava kreditne kartice Diners' Cluba 1951., prvog bankomata Barclaysa 1967., prve internetske stranice za bankarstvo The Stanford Credit Uniona 1994. godine te prvog pametnog telefona iPhone-a 2007. godine koji je potpuno promijenio način bankarskog poslovanja, a time i cjelokupnog platnog prometa samo su neki od primjera iz povijesti digitalizacije bankarstva koji su zauvijek promijenili živote većine ljudi na svijetu. Za sve navedene primjere možemo reći da imaju jednu stranu zajedničku – da se od pojave ovakvih revolucionarnih izuma, također, pronalaze ilegalni načini kako iste izume prevariti, kompromitirati i učiniti manje sigurnim na teret korisnika i pružatelja usluge zbog koristi treće strane. Možemo reći kako se sigurnost bankarskih informacijskih sustava, a time i cjelokupnog platnog prometa nije razvijala dovoljno brzo te su se ljudi tek nakon velikih internetskih napada (eng.*cyber attack*), prijevara i skandala osvijestili i dali važnost problemima sigurnosti bankarskih informacijskih sustava. Tek su se u nedavnoj povijesti donijele brojne regulative, tehnološki standardi te propisali zakoni kako bi se trebao štititi cjelokupni platni promet od neželjenih sigurnosnih napada. Predmet ovog rada je analiza utjecaja sigurnosnih mjera platnog prometa prije te po nastupanju COVID-19 krize (pandemije) te kako je primjena donesenih mjera utjecala na sigurnost platnog prometa.

Cilj rada je na temelju analiza rizika i provedenog istraživanja donijeti zaključak o utjecaju i uspješnosti sigurnosnih mjera na cjelokupnu sigurnost platnog prometa u doba COVID-19 pandemije. Također, cilj je rezultate dobivene istraživanjem percepcije korisnika o zaštiti bezgotovinskih plaćanja usporedit će se s rezultatima sličnih istraživanja, kako bi se potvrdio trend i vjerodostojnosti istraživanja. Proces rada započinje definiranjem i objašnjenjem pojmova važnih za razumijevanje rada. U sljedećem koraku opisat će se okruženja prije u vrijeme pandemije. Nakon objašnjenog okruženja identificirat će se rizici nastali prije i u vrijeme COVID-19 pandemije te kako su se odrazili na cjelokupnu sigurnost platnog prometa. U nastavku rada sistematizirano će biti prikazane sigurnosne mjere, smjernice i napuci kako od strane brojnih domaćih i europskih regulatornih ustanova, tako i od strane banaka, velikih kartičnih kuća i ostalih financijskih institucija.

U posljednjem dijelu rada naglasak će biti na istraživanju i percepciji korisnika o sigurnosti bezgotovinskih transakcija u doba krize. Proces i prikupljanje podataka odnosi se na razdoblje od kraja 2019. godine i početka COVID-19 pandemije 2020. sve do kraja 2021. godine. Rezultati istraživanja oblikovat će konačan zaključak o uspješnosti donesenih mjera koje su trebale osigurati sigurnu i neometanu provedbu te procesuiranje bezgotovinskih transakcija kao i funkcioniranje cjelokupnog platnog prometa. Znanje i metode koje će se koristiti u radu stečeni su na kolegijima Revizija informacijskih sustava, Elektroničko poslovanje te Upravljanje rizicima.

Stručni doprinos ovog rada odražava se u identificiranju svih rizika, te pronalasku važnih donesenih mjera za sigurnost platnog prometa i njihovoj uspješnosti u zaštiti sigurnosti cjelokupnog platnog prometa. Stručno doprinos očituje se i u provedbi istraživanja o percepciji korisnika o zaštiti bezgotovinskih transakcija te usporedbi rezultata i interpretiranje sa sličnim radovima i istraživanjima za vrijeme pandemije, koji su obzirom da aktualnost teme prilično oskudna. Važno je istaknuti razumijevanje aktualnosti vremena i važnosti primjene stečenih znanja te prepoznavanja značajnosti rizika platnog prometa u iznenadnim situacijama s malom vjerojatnošću nastupanja. Analiza i rezultati istraživanja percepcije korisnika o sigurnosti bezgotovinskih transakcija, kao primarnom načinu stjecanja dobra u doba pandemije kao i mnogobrojne mjere zaštite donesene od važnih institucija, potvrdit će tezu o uspješnosti zaštite platnog sustava uslijed razdoblja COVID-19 panedmije.

1.2 Izvori i metode prikupljanja podataka

Teorijska podloga za pisanje ovog rada su brojni sekundarni izvori domaćih i stranih podataka prije svega postojeća stručna i znanstvena literature, brojni časopisi, aktualne publikacije, članci i istraživanja relevantna za temu sigurnosti informacijskih sustava, platnog prometa te bezgotovinskih transakcija.

U okviru istraživanja koristili su se primarni izvori podataka prikupljeni provedenom anketom na društvenoj mreži Facebooku u razdoblju od 12. do 19. srpnja 2021. godine. Dobiveni podaci su obrađeni i analizirani. Na temelju dobivenih rezultata donesen je vjerodostojan zaključak percepcije korisnika o sigurnosti bezgotovinskih transakcija u doba COVID-19 pandemije.

1.3 Struktura rada

Rad se sastoji od pet cjelina. U uvodnom dijelu se kratkim i najznačajnijim trenucima iz prošlosti sigurnosti bankarskog poslovanja pokušava objasniti problem, cilj i okvir teme ovoga rada. U drugom poglavlju definiraju se pojmovi platnog prometa, sigurnosti informacijskih sustava i bezgotovinskih transakcija. Ovi pojmovi izrazito su značajni za kvalitetno razumijevanje problema i cilja rada. U trećem poglavlju definirat će se okruženje prije i za vrijeme nastale pandemije te probleme koje je uzrokovala za pojedinca i financijsko tržište. U četvrtom poglavlju analizirat će se glavni sigurnosni rizici platnog prometa nastalih u COVID-19 pandemiji i način na koji su se štitile transakcije između pravnih osoba, fizičkih osoba, te pravnih i fizičkih osoba.

2. Platni promet i sigurnosni aspekti informacijskog sustava platnog prometa

2.1 Platni promet

„Platni promet se sastoji od seta instrumenata, procedura, pravila i tehničke potpore za slanje informacija i namiru transakcija između sudionika. Neizostavan je dio gospodarskog sustava svake zemlje i njegova je temeljna funkcija omogućavanje sigurne i učinkovite uporabe novca kao sredstva plaćanja kao i izvršavanje bezgotovinskih platnih transakcija odnosno prijenos sredstava od platitelja primatelju plaćanja“ (HNB, 2020.).[1] „U užem smislu, platni promet obuhvaća formalne aranžmane temeljene na ugovorima i zakonodavstvu, sa standardiziranim pravilima i ugovornim odnosima za slanje, kliring i namiru obaveza i instrumenata između sudionika. Pružatelji platnih usluga jesu kreditne institucije, institucije za elektronički novac, male institucije za elektronički novac, institucije za platni promet, male institucije za platni promet i registrirani pružatelji usluge informiranja o računu. Platni promet u Republici Hrvatskoj izvršava se preko pet platnih sustava, a to su: Hrvatski sustav velikih plaćanja (HSVP), Nacionalni klirinški sustav (NKS), NKSInst, TARGET2, EuroNKS“ (HNB, 2020).[2] Zakonu o platnom prometu definira, kako se platni promet sastoji se od: platnih usluga i njihovi pružatelji, obveze pružatelja platnih usluga, institucije za platni promet i platni sustavi.[3]

[1] HNB (2020.), O platnom prometu, preuzeto 30. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/o-platnom-prometu
[2] HNB (2020.), Što je platni promet?, pruzeto 20. rujna 2021. s https://www.hnb.hr/-/sto-je-platni-promet-
[3] Zakon o platnom prometu, Narodne novine br. 66/2018. (2018.)

Prema Europskoj centralnoj banci „Platni promet je sustav plaćanja koji uključuje infrastrukturu financijskog tržišta za plaćanja, vrijednosne papire i izvedenice te je temeljna komponenta financijskog sustava uz tržišta i institucije. Uloga platnog prometa je efikasno i sigurno izvršavanje transakcije među gospodarskim subjektima što je preduvjet za neometano funkcioniranje suvremenih gospodarstava“ (ECB, 2010.).[4]

2.2 Platni Promet u Republici Hrvatskoj

„Platni promet u Republici Hrvatskoj izvršava se preko pet platnih sustava, a to su: Hrvatski sustav velikih plaćanja (HSVP), Nacionalni klirinški sustav (NKS), TARGET2, EuroNKS“ (HNB, 2015.).[5]

Hrvatski sustav velikih plaćanja (HSVP)

„Hrvatski sustav velikih plaćanja platni je sustav u kojemu se platne transakcije u kunama namiruju u realnom vremenu u bruto načelu, a riječ je o uglavnom relativno velikim iznosima. Platne transakcije provode su u svrhu provođenja mjera monetarne politike HNB-a, u svrhu opskrbe banaka gotovim novcem, u svrhu provođenja namire drugih platnih sustava i ostale platne transakcije. Sudionici HSVP-a jesu Hrvatska narodna banka, kreditne institucije (banke i štedne banke) sa sjedištem u Republici Hrvatskoj, Hrvatska banka za obnovu i razvitak te Središnje klirinško društvo“ (HNB, 2015.).[6]

Nacionalni klirinški sustav (NKS)

„Nacionalni klirinški sustav je međubankovni platni sustav za multilateralni obračun po neto načelu većeg broja platnih transakcija u kunama koje glase na relativno male iznose. NKS omogućuje obračun bezgotovinskih međubankovnih platnih transakcija u kunama svih

[4] ECB (2010.), The payment system – payments, securities and derivatives, and the role of eurosystem, preuzeto 30. kolovoza 2021. s https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf
[5] HNB (2015.), O platnom prometu, preuzeto 30. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/o-platnom-prometu
[6] HNB (2015.), Hrvatski sustav velikih plaćanja, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/hsvp

sudionika NKS-a. Sudionici NKS-a jesu HNB, kreditne institucije (banke i štedne banke) te Hrvatska banka za obnovu i razvitak. Upravitelj i vlasnik NKS-a je Fina“ (HNB, 2015.).[7]

TARGET2

„TARGET2 (engl. *Trans – European Automated Real – Time Gross settlement Express Transfer system*) platni je sustav za namiru platnih transakcija u eurima u realnom vremenu na bruto načelu. To je sustav s jedinstvenom tehničkom platformom – eng. *Single Shared Platform* (SSP) kojom zajednički upravljaju u ime Eurosustava Banca d'Italia, Banque de France i Deutsche Bunedsbank. Europska središnja banka glavno je nadzorno tijelo sustava TARGET2. Program su razvile središnje banke EU-a s ciljem sigurne i efikasne namire platnih transakcija (nacionalnih i prekograničnih) u eurima na RTGS načelu (eng. *Real Time Gross Settlement*) te olakšava provođenje monetarne politike EU-a“ (HNB, 2015.).[8]

EuroNKS

„EuroNKS platni je sustav koji obrađuje međubankovne platne transakcije SEPA kreditnih transfera u eurima. Financijska agencija Fina odgovorna je za realizaciju, uspostavu i operativno upravljanje infrastrukturom EuroNKS. U EuroNKS-u banke imaju otvorene obračunske račune u eurima, a sustav obrađuje međubankovna eurska plaćanja SEPA kreditnih transfera koja su u potpunosti usklađena sa zahtjevima iz Uredbe (EU) br. 260/2012“ (HNB, 2015.).[9]

2.3 Sigurnost informacijskih sustava i *Cyber* sigurnost

Sigurnost informacijskih sustava i *cyber* sigurnost do nedavno su bile teme o kojima se nije puno govorilo. No uz sve brži tehnološki razvoj razvila se i većina sigurnosnih prijetnji koje su se nekada činile kao nezamislive, a danas su skoro pa uobičajene. Veliki propusti u sigurnosti informacijskih sustava i *cyber napadi* su se dogodili u zadnjih deset godina, upravo iz razloga

[7] HNB (2015.), Nacionalni klirinški sustav, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/nks
[8] HNB (2015.), TARGET2, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/target2
[9] HNB (2015.), EuroNKS, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/euronks

što se većina čini nemogućim te im se iz tog razloga nije pridavalo puno pažnje. Tek onda kada su nastupili i kada su velike organizacije pretrpjele goleme novčane gubitke, kako od samih sigurnosnih propusta tako i zbog kazni regulatora, sigurnosti informacijskim sustava i *cyber* sigurnosti se počela pridavati sve veća pažnja, prije svega naglasak je na sprječavanju pojave, i ukoliko se one dogode ublažavanju posljedica takvih pojava.

„Sigurnost informacijskih sustava definira se kao skup metoda i zaštitnih mjera (kontrola) kojima se informacije i informacijski sustavi štite od neovlaštenog: pristupa, uporabe, otkrivanja, prekida rada, promjena ili uništenja“ (Spremić, 2017.).[10] „Pojavom interneta započelo i sve veće automatiziranje svakodnevnih ljudskih poslova. Uz razvoj promjena koje su se dogodile u međuljudskim komunikacijama svakako treba vezati i pojam računalnih mreža. Računalne mreže postale su glavni prijenosnik informacija i povezivanja ljudi u cijelome svijetu“ (Bača, 2004.).[11] „U poslovnom svijetu sve više počele koristiti tehnologije zasnovane na internetu te digitaliziranje usluga koje klijentima nude veću vrijednost i bolje iskustvo poslovanja, s druge strane kriminalci konstantno pronalaze nove načine kako iste sustave kompromitirati i učiniti manje sigurnim. Što je tehničko savršenstvo računala veće, uz istovremeno pojednostavljenje njihove upotrebe, to su i veće mogućnosti za njegovu zloupotrebu“ (Bača, 2004.).[12] Iz navedenog možemo reći kako je danas jedan od najvažnijih preduvjeta te okosnica uspješnog i održivog poslovanja upravo zaštita informacijskih sustava od narušavanja povjerljivosti i bilo kakve ugroze podataka klijenata.

„Pojam *Cyber* sigurnosti odnosi se na holistički model ovladavanja, upravljanja i osiguravanja funkcioniranja suvremenoga informatičkog okruženja koji uključuje: tehnološke, organizacijske, društvene, i ostale aspekte, u odnosu na klasične procedure informacijske sigurnosti koje su mahom tehnološki usmjerene. *Cyber* sigurnost je pojam koji se usredotočuje na specifične, visoko sofisticirane metode napada i pokriva organizacijske, tehnološke i socijalne društvene aspekte napada. Možemo reći kako je glavni cilj kontrolnih mjera *cyber* sigurnosti sprječavanje pojave ili ublažavanje posljedica koje stalne (neodgodive) prijetnje, *cyber* ratovi i *cyber* napadi mogu imati na pojedince i kompanije“ (Spremić, 2017.).[13] ISACA (eng. *Information System Audit and Control Association*) *cyber* sigurnost definira „kao zaštitu

[10] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb: Ekonomski fakultet
[11] Bača, M. (2004.), Uvod u računalnu sigurnost, Narodne novine, Zagreb
[12] Bača, M. (2004.), Uvod u računalnu sigurnost, Narodne novine, Zagreb
[13] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb: Ekonomski fakultet

informacijskih resursa utvrđivanjem prijetnji informacijama koje se obrađuju, pohranjuju i prenose međusobno povezanim informacijskim sustavima“ (ISACA, 2014.).[14]

2.4 Bezgotovinske transakcije

Kada se spominju bezgotovinske transakcije danas ljudi prvo pomisle na transakcije koje se odvijaju putem debitnih, kreditnih ili *charge* kartica, digitalnog novčanika, kriptovaluta te raznih aplikacija za mobilno ili internet bankarstvo. Ukoliko bolje razmislimo brzo shvaćamo da one postoje već jako dugo vremena. Najbolji primjer za bezgotovinske transakcije u bližoj povijesti su čekovi koje su garantirali isplatu novca onome tko ih donese u banku.

„Preduvjet obavljanja bezgotovinskih transakcija (elektroničkih) kakve danas najčešće koristimo i poznajemo bio je razvoj tehnologije elektroničkog sustava plaćanja i elektroničkog novca. Elektronički sustav plaćanja postoji od šezdesetih godina prošlog stoljeća te od razvoja sustava elektroničkog prijenosa novca (engl. Electronic Funds Transfer – EFT), koji je postajao sve sofisticiraniji te se upotrebljavao u sve većem broju zemalja. EFT implicira primjenu računalne i telekomunikacijske tehnologije pri plaćanju. Navedenim su se sustavom koristile banke i druge financijske institucije kako bi razmjenjivale i prenosile velike količine novca na nacionalnoj i međunarodnoj razini. Osnova funkcioniranja EFT-a jest da se novac kreće putem mreža kao supstitut gotovine ili čekova kako bi se obavila transakcija. Zadaća sustava jest skratiti vrijeme plaćanja te smanjiti transakcijske troškove“ (Hamdi, 2007.).[15] Tek devedesetih godina prošloga stoljeća bezgotovinske transakcije su postale učestalije zbog sve bržeg informatičkog razvitka što je rezultiralo smanjenjem cijena računala i njihovom širom primjenom.

Bezgotovinske transakcije (elektroničke) danas su usko vezane uz pojam elektroničkog novca te je iz tog razloga važno da razumijemo njegov koncept. „Elektronički novac možemo definirati kao novac koji jest elektronički, uključujući i magnetski, pohranjena novčana vrijednost koja je izdana nakon primitka novčanih sredstava u svrhu izvršavanja platnih transakcija u smislu zakona kojim se uređuje platni promet i koju prihvaća fizička ili pravna osoba koja nije izdavatelj toga elektroničkog novca, a koja čini novčano potraživanje prema izdavatelju“ (NN, 2008.).[16] Prema Europskoj centralnoj banci elektronički novac je „novčana

[14] ISACA (2015.), Global Cyber Security Status Report, ISACA, Roling Meadows, Illinois, USA
[15] Hamdi, H. (2007.), Problemi razvoja elektroničkog novca, Financijska teorija i praksa 31(3), 291. str. https://hrcak.srce.hr/18214
[16] Zakon o elektroničkom novcu, Narodne novine br. 66/2018., (2018.)

vrijednost, predstavljena potraživanjem od izdavatelja, koja je: pohranjena na elektroničkom uređaju (npr. kartici ili računalu), izdana po primitku sredstava u iznosu koji nije manji od primljene novčane vrijednosti i prihvaćeni kao sredstvo plaćanja od strane društava osim izdavatelja“ (ECB, b.d.).[17] Dakle, bezgotovinske transakcije možemo definirati kao prijenos elektroničkog novca s računa platitelja na račun primatelja.

3. Poslovno okruženje prije i u vrijeme COVID-19 pandemije

3.1 Okruženje prije pandemije

„Financijska kriza koja se dogodila 2008. godine, najgora u posljednjih sedamdeset godina, koja je utjecala na ekonomiju cijeloga svijeta te zauvijek promijenila način na koji živimo. Neki od primjera poput načina na koji ljudi i institucije ulažu, stavke koje centralne banke reguliraju te pod kojim uvjetima banke kreditiraju stanovništvo dovoljno ukazuju na ozbiljnost posljedica krize“ (Wenjie, Mrkaic i Nabar, 2019.).[18] Od krize 2008. pa sve do kraja 2019. godine možemo reći da je uslijedilo razdoblje sporijeg, ali relativno konstantnog rasta svjetske ekonomije. „Regulatori diljem svijeta poduzeli su određene mjere kako bi banke učinili što otpornijima od budućih financijskih šokova. Stopa obvezne rezerve s manje od 4 posto 2007. godine na jednako ili više od 15 posto u 2017. godini za američke i europske banke“ (Lundt i sur., 2018.).[19]

„Važno je spomenuti kako se u doba nakon krize počelo koristiti sve više novih tehnologija, koje su olakšavale izvršavanje transakcija te time ubrzale digitalizaciju cijelog društva. Najbolji primjer je sve veća primjena rada u oblaku (eng. *cloud*) koji se temelji na pohrani podataka koja nije lokalna, već je arhivirana na serveru kojem se pristupa preko internetske veze koja omogućuje da se podacima pristupa bilo gdje na svijetu kada su nam oni potrebni što otvara brojne mogućnosti u inovaciji poslovanja“ (Berman i sur., 2012.).[20] Jedan od najvažnijih izuma

[17] ECB (b.d.) Electronic money, preuzeto 31. kolovoza 2021. s https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

[18] Wenjie, C., Mrkaic. M., Nabar, S., M. (2019.), The Global Economic Recovery 10 Years After the 2008 Financial Crisis, preuzeto 1. rujna 2021. s https://www.imf.org/en/Publications/WP/Issues/2019/04/26/The-Global-Economic-Recovery-10-Years-After-the-2008-Financial-Crisis-46711

[19] Lund, S., Mehta, A., Manyka, J., Goldshtein, A. (2018.), A decade after the global financial crysis: What has (and hasn't) changed?, preuzeto 2. rujna 2021. s https://www.mckinsey.com/industries/financial-services/our-insights/a-decade-after-the-global-financial-crisis-what-has-and-hasnt-changed

[20] Berman, S., J., Kesterson-Townes, L., Marshall, A., Sirvathsa, R. (2012.), How cloud computing enables process and business model innovation, preuzeto 2. rujna 2021. s https://www.emerald.com/insight/content/doi/10.1108/10878571211242920/full/html

koji je doživio široku primjenu diljem svijeta svakako je izum pametnih telefona, koji je rezultirao da ljudi više vremena provode na mobitelu radeći stvari za koje im je prije bilo potrebno stolno ili prijenosno računalo. Takvo ponašanje su rano uvidjele banke i ostale financijske institucije, obzirom da su na taj način svojim korisnicima mogli ponuditi bolje iskustvo poslovanja, koji nisu primorani stalno dolaziti u poslovnicu kako bi napravili uplatu ili riješili određeni problem već to mogu napraviti bilo gdje, dokle god sa sobom imaju pametni telefon i internetsku vezu. O tome koliko su pametni telefoni promijenili način poslovanja financijskih institucija i preferencije obavljanja transakcija kod ljudi najbolje svjedoči podatak HNB-a o povećanju vrijednosti bezgotovinskih transakcija u zadnjih pet godina.

„U zadnjih pet godina bezgotovinske platne transakcije povećale su se za 58 posto, dok se njihova vrijednost povećala za 47 posto. Također, u porastu je broj obavljenih transakcija putem mobilnog bankarstva. Dosadašnjem porastu bezgotovinskih platnih transakcija uvelike je pridonosio razvoj internetskoga i mobilnog bankarstva kao i razvoj kartičnih plaćanja“ (Mišić, 2020.).[21] „Na dan 31. prosinca 2019. godine 32 posto potrošača i 27 posto poslovnih subjekata u RH imalo je ugovorenu uslugu mobilnog bankarstva. U odnosu na broj korisnika mobilnog bankarstva na dan 31. prosinca 2018. broj korisnika mobilnog bankarstva potrošača u 2019. povećao se za 24 posto, a poslovnih subjekata za 91 posto. U RH u 2019. Potrošači su u 2018. godini napravili 29,7 milijuna transakcija korištenjem usluge internetskog bankarstva u ukupnoj vrijednosti od 30 milijarda kuna dok su u 2019. godini napravili 61,3 milijuna transakcija korištenjem usluge mobilnog bankarstva u ukupnoj vrijednosti od 46,7 milijarda kuna“ (HNB, 2020.).[22]

Razvoj pametnih telefona pratilo je i razvijanje novih metoda kriptiranja podataka korisnika kao i autentikacijskih metoda kojima korisnici potvrđuju svoj identitet prilikom plaćanja. Korištenje jednokratne zaporke, tokena ili mtokena samo su neke od metoda koje se široko primjenjuju od pojave pametnih telefona i internetske kupovine pri obavljanju bezgotovinskih transakcija. „U zadnjih nekoliko godina uspješno je integriran način potvrde identiteta putem biometrijskih metoda, poput otiska prst ili skeniranja lica korisnika. Danas se najsigurnijim oblikom autentikacije ipak smatra multifaktorska autentikacija koja je kombinacija

[21] Mišić., T. (2021.), Utjecaj pandemije COVID-19 na navike plaćanja u RH, preuzeto 1. rujna 2021. s https://www.hnb.hr/-/utjecaj-pandemije-covid-19-na-navike-placanja-u-rh

[22] HNB (2021.), *Ukupna vrijednost bezgotovinskih transakcija u pet se godina povećala za 47 posto* [e-publikacija], preuzeto s: https://www.hnb.hr/analize-i-publikacije/redovne-publikacije/bezgotovinske-platne-transakcije

biometrijskih s klasičnom metodama temeljenih na znanju korisnika, poput PIN-a ili jednokratne zaporke“ (Teh i sur., 2016.).[23]

3.2 Utjecaj COVID-19 pandemije na društvo i poslovanje

COVID-19 pandemija najveća je kriza suvremenog doba koja je u kratkom vremenu utjecala na cijeli svijet te se u određenoj mjeri odrazila na život svakog čovjeka. „Program za razvoj Ujedinjenih naroda COVID-19 pandemiju opisao je kao ključnu zdravstvenu krizu našeg vremena i najveći izazov s kojim smo se suočili od Drugog svjetskog rata. Od svog nastanka u Aziji krajem prošle godine, virus se proširio na sve kontinente, osim na Antarktiku“ (UN, 2020.).[24] „Kao geografsko središte pojave COVID-19 virusa obilježava se grad Wuhan u Narodnoj republici Kini od kuda se dalje proširio u ostale gradove i kontinente što potvrđuje istraživanje Svijetske zdravstvene organizacije iz 2020. godine“ (WHO, 2021.).[25] Obzirom da se radio o novom obliku virusa koji se brzo širi, u svijetu su ubrzo poduzete stroge mjere u borbi protiv virusa poput velikih zatvaranja (eng. *lockdown*) svih poduzeća, prodajnih mjesta i ustanova osim dućana za nabavu hrane te proizvoda široke potrošnje. Većina tvornica u doba najtežeg dijela pandemije i *lockdowna* nije proizvodilo što se u povijesti još nikada nije dogodilo te je na par tjedana paralizirano gospodarstvo cijeloga svijeta. Pandemija uzrokovana virusom nije samo zdravstvena, već ponajprije socijalna i ekonomska kriza. „Glavni direktor WHO-a navodi kako su svjetski gubici uzrokovani pandemijom veći od 375 milijardi američki dolara mjesečno, a kumulativni gubitak predviđa se na oko 12 trilijuna američkih dolara“ (WHO, 2020.).[26] Važno je i spomenuti kako je kriza uvelike utjecala i na ponašanje te mentalno stanje ljudi. Zbog donesenih mjera zaštite od virusa u cijelome svijetu svakodnevne obveze ubrzano su organizirane na drugačiji način, poput rada od kuće i školovanja preko *online* oblika nastave što je zahtijevalo prilagodbu na „novo normalno“. Utjecaji zbog *lockdowna*, socijalne

[23] Teh, P.S., Zhang, N. Teoh, A.B.J. and Chen, K. (2016), TDAS: a touch dynamics based multi-factor authentication solution for mobile devices, *International Journal of Pervasive Computing and Communications*, Vol. 12 No. 1, pp. 127-153. https://doi.org/10.1108/IJPCC-01-2016-0005

[24] United Nations Development Programme (2020.), COVID-19 pandemic, preuzeto 1. rujna 2021. s https://www.pacific.undp.org/content/pacific/en/home/coronavirus.html

[25] World Health Organization (2021.), Global Study of Origins of SARS-CoV-2: China Part, preuzeto 1. rujna 2021. s https://www.who.int/publications/i/item/who-convened-global-study-of-origins-of-sars-cov-2-china-part

[26] World Health Organization (2020.), WHO Director-General's opening remarks at the media briefing on COVID-19 - 13 August 2020, preuzeto 2. rujna 2021. s https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---13-august-2020

izolacije, straha od gubitka prijatelja i članova obitelji samo su neki od mnogih koji su rezultirali povećanjem depresije i tjeskobe te općenito lošeg mentalnog stanja kod ljudi.

3.3 Poslovno okruženje u doba pandemije

3.3.1 Internetska kupovina i bezgotovinske platne transakcije

Zbog nastale situacije uzrokovane COVID-19 virusom i njegovim utjecajem na svjetsko tržište, a time i na život svakog čovjeka značajne promijene mogu se učiti u ponašanju potrošača prilikom internetske kupovine i bezgotovinskih plaćanja u doba pandemije. „U Sjedinjenim Američkim Državama 17 posto potrošača odlučilo se za drugačiju trgovinu od trgovine u kojima su primarno kupovali, obzirom da su trgovine koje do pandemije nisu imale, otvorile i internetske trgovine. „Mnogi potrošači isprobali su i neke nove modele kupovine, poput kupnje u internetskoj trgovini i preuzimanja predmeta u fizičkoj trgovini, tzv. BOPIS (eng. *buy online, pick up in store)* te je takav način internetske kupovine porastao za 28 posto u veljači u odnosu na 18 posto iz siječnja prethodne godine. Također, porast se dogodio i u dostavi namirnica i robe široke potrošnje, koji je u veljači bio 57 posto veći nego u siječnju prethodne godine. Najsuvremeniji trgovci proveli su godine usavršavajući spajanje fizičke i online trgovine kako bi privukli potrošače. Utjecaj pandemije na kupaca dramatično je promijenio njihovo ponašanje te se tako osobna interakcija zamijenila digitalnom te svi pokazatelji upućuju da bi tako moglo ostati trajno. Prodaja u internetskim trgovinama odjeće, kozmetike u prosijeku je porasla za gotovo 10 posto od početka pandemije. U trgovini mješovitom robom internetska prodaja porasla je s 2 na 3 posto prije krize na 8 do 10 posto na svojemu vrhuncu te se očekuje da će se do kraja godine smiriti na dvostruko većoj „normalnoj“ razini od 5 do 7 posto“ (Briedis i sur., 2020.).[27] „U zemljama Europske unije prevladavaju slična kretanja. Prema OECD-u (2020.) u EU-27 zemljama, internetska prodaja u travnju 2020. godine povećala se za 30 posto u odnosu na travanj 2019. godine, dok se ukupna prodaja u fizičkim trgovinama smanjila za 17.9 posto. Rezultati zamijene fizičkih trgovina s internetskim vrlo je vjerojatna i u ostalim zemljama“ (OECD, 2020.).[28]

[27] Briedis H., Ungerman K., Kronschnabl A., Rodriguez A. (2020.), Adapting to the next normal on retail: The Customer experience imperative, preuzeto 2. rujna 2021. s https://www.mckinsey.com/industries/retail/our-insights/adapting-to-the-next-normal-in-retail-the-customer-experience-imperative

[28] OECD (2020.), *E-commerce in the time of COVID-19* [e-publikacija], preuzeto s https://read.oecd-ilibrary.org/view/?ref=137_137212-t0fjgnerdb&title=E-commerce-in-the-time-of-COVID-19&_ga=2.62472940.1345077669.1630588043-2051317201.1630494535

Bezgotovinske platne transakcije bile su u porastu i prije COVID-19 pandemije zbog sve bržeg razvoja kartičnih plaćanja te sve važnijeg razvoja mobilnog i internetskog bankarstva. U pandemiji su najviše korištena bezgotovinska sredstva plaćanja bile kartice. Na vrhuncu pandemije kada su donesene mjere o *lockdownu* te je strah ljudi od zaraze virusom bio velik ljudi su počeli više koristiti beskontaktni oblik kartičnog plaćanja. Sve veće korištenje beskontaktnih plaćanja potvrđuje i podatak Hrvatske narodne banke „kako je u Republici Hrvatskoj na dan 31. ožujka 2020. godine od ukupnog broja platnih kartica njih 55 posto bilo beskontaktno, dok je od ukupnog broja EFTPOS (eng. *electronic funds transfer on point of sale*) uređaja njih čak 80 posto omogućavalo iniciranje beskontaktnih platnih transakcija" (HNB, 2021.).[29] Razlog povećanju broja kartičnih beskontaktnih transakcija ujedno je i povećanje limita za beskontaktne transakcije krajem travnja 2020. godine. „Hrvatska narodna banka je, kako bi se u uvjetima mjera Stožera potrošačima omogućilo izvršenje plaćanja bez fizičkoga kontakta, bankama i kartičnim kućama dala preporuku povećanja maksimalnog iznosa beskontaktne platne transakcije bez upotrebe PIN-a s tadašnjih 100,00 kuna na 250,00 kuna. Povećanje maksimalnog iznosa imalo je snažan utjecaj s obzirom na to da su kartice s beskontaktnom funkcijom u RH već tada činile većinu izdanih platnih kartica te su u obavljanju svakodnevnih transakcija već bile iznimno zastupljene uz iznimno dobru prihvaćenost kod korisnika" (Mišić, 2021.). [30]

Povećani trend korištenja bezgotovinskih kartičnih transakcija možemo vidjeti i u ostalim zemljama svijeta. „Prema Švicarskoj nacionalnoj banci postotak platnih transakcija putem debitnih kartica povećao se s 65 posto na 72 posto između siječnja i svibnja 2020. godine" (Švicarska narodna banka, 2020.).[31] „Bruno, Denecker i Niederkorn također navode kako je jedan od bitnijih razloga porasta broja beskontaktnih kartičnih transakcija povećanje limita beskontaktnih kartičnih transakcija" (Bruno, Dencker i Niederkorn, 2020.).[32]

[29] HNB (2021.), Platne kartice i kartične transakcije, [e-publikacija], preuzeto 3. rujna 2021. s https://www.hnb.hr/analize-i-publikacije/redovne-publikacije/platne-kartice-i-karticne-transakcije

[30] Mišić., T. (2021.), Utjecaj pandemije COVID-19 na navike plaćanja u RH, preuzeto 3. rujna 2021. s https://www.hnb.hr/-/utjecaj-pandemije-covid-19-na-navike-placanja-u-rh

[31] Swiss National Bank (2020.), Payments and cash withdrawals, preuzeto 3. rujna 2021. s https://data.snb.ch/en/topics/finma#!/cube/zavezaka?fromDate=2020-01&toDate=2021-01&dimSel=D0(T0,DZ0,T1,DZ1)

[32] Bruno, P., Dencker, O., Niederkorn, M. (2020.), Accelerating winds of change in global payment, preuzeto 3. rujna 2021. s https://www.mckinsey.com/industries/financial-services/our-insights/accelerating-winds-of-change-in-global-payments

4. Sigurnosni aspekti platnog prometa u doba COVID-19 pandemije

4.1 Identifikacija i analiza sigurnosnih rizika

Kako bismo bolje razumjeli *cyber* rizike, a time i sigurnosne rizike platnog prometa potrebno je prije svega definirati i razumijeti koncept i definiciju samog rizika i njegovog utjecaja na cjelokupnu sigurnost poslovanja.

„Opća definicija rizika polazi od vjerojatnosti nastanka događaja koji će imati negativne posljedice na pojedinca, organizaciju, ili društvo u cjelini“ (Miloš Sprčić, 2013.).[33] „U svojoj knjizi s aspekta poslovnih rizika, rizik definira kao vjerojatnost nastupanja određenih događaja koji će imati negativne učinke na vrijednost očekivanih zarada, novčanih tokova, i vrijednost poduzeća, odnosno koji će ugroziti njezine poslovne ciljeve“ (Culp, 2001.).[34]

„Pojam *cyber* rizika odnosi se na rizik koji predstavlja opasnost ili vjerojatnost da će odgovarajući izvor prijetnje u određenim okolnostima iskoristiti ranjivost (slabost) sustava, čime se, posljedično, može počiniti neka šteta imovini organizacije. *Cyber* rizici (informatički rizici) su poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije u okruženju digitalne ekonomije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i poslovanja uopće. Najvažniji čimbenici upravljanja informatičkim rizicima se odnose na učestalost pojave i utjecaj na poslovanje. Informatički i *cyber* rizici proizlaze iz djelovanja prijetnji. Prijetnje se obično dijele s obzirom na mjesto nastanka pa razlikujemo unutarnje (interna prijevara, neovlašten pristup informacijama iznutra, krađa resursa informacijskog sustava) i vanjske (hakerski napadi, zlonamjerni računalni kod, društveni inženjering, epidemije i bolesti, elementarne nepogode). Identificirane prijetnje potrebno je staviti u kontekst ranjivosti resursa informacijskog sustava, koje pojedine prijetnje mogu iskoristiti te na taj način izazvati štetni učinak. Neki od primjera ranjivosti su: nepostojanje zaštite od malicioznoga koda, neprimjerena konfiguracija vatrozida, zaposlenici koji imaju nisku razinu svijesti o sigurnosti informacijskog sustava.

Poznavanjem ranjivosti, prijetnji i njihovih štetnih učinaka na poslovanje mogu se procijeniti rizici informacijskog sustava kroz njihova dva temeljna svojstva: vjerojatnost da će prijetnja

[33] Miloš Sprčić, D. (2013.), Upravljanje rizicima – temeljni koncepti, strategija i instrumenti, Zagreb, Sinergija
[34] Culp, L., C. (2001.), The Risk Management Process – Business Strategy, and Tactics, John Wiley & Sons

iskoristiti ranjivost resursa informacijskog sustava i razina štetnog učinka ako prijetnja uspješno iskoristi ranjivost“ (Spremić, 2017.).[35]

U doba pandemije ističu se dvije vrste informatičkih rizika koji su se najčešće događali i time utjecali na informatičku sigurnost cjelokupnog platnog prometa. „Rizici provedbe poslovnih procesa ili transakcijski informatički rizici su svi rizici primjene informacijske tehnologije u redovitoj provedbi poslovnih procesa. U ovu kategoriju možemo nabrojati sve operativne informatičke rizike na koje treba obratiti pozornost kako bi se poslovni procesi mogli izvoditi na neometan, siguran i pouzdan način. Neki od primjera ovih rizika su: sigurnosni informatički rizici, rizici neprekidnosti poslovanja, rizik provedbe poslovnih transakcija (jesu li transakcije točne, potpune, cjelovite), rizik ometanja ili prekida poslovnih transakcija, rizik integriteta, rizik nedostupnosti sustava, rizik oporavka nakon neželjenog napada. Druga Važna vrsta rizika su infrastrukturni informatički rizici koji predstavljaju rizik rada informatičke infrastrukture. Ti rizici se odnose i na dostupnost i funkcionalnost računalne mreže, komunikacijsku infrastrukturu te ostalih servisa koje poduzeće pruža“ (Spremić, 2017.).[36] Obzirom da *cyber* rizici proizlaze iz prijetnji, u 2020. godini dogodila se upravo vanjska prijetnja za koju se mislilo da je gotovo nemoguće da se dogodi – pandemija uzrokovana do tada nepoznatim virusom. Upravo je pandemija bila „okidač“ za niz rizika koji su uslijedili i nepovoljno utjecali na cjelokupnu sigurnost platnog prometa. U doba kada je pandemija zahvatila većinu svijeta te postepenim zatvaranjem (eng. *lockdown*) sve je više rasla značajnost skupine rizika od provedbe poslovnih procesa, obzirom da je način rada i izvršavanja usluga putem interneta sve više rastao. Dobar primjer koji pripada toj skupini rizika je rizika neprekidnosti poslovanja. Rizik neprekidnosti poslovanja ima izniman utjecaj na izravnu dobit poduzeća. Ukoliko jedan dio sustava ne radi, tada sve komponente sustava ne rade te se vrijednost štete povećava iz minute u minutu zbog nemogućnosti pružanja usluga, provedbe transakcija i naloga. „Kao primjer manifestacije ovog rizika možemo navesti jednu od najvećih osiguravajućih kuća u SAD-u, CNA koja je prema Bloombergu napadnuta zloćudnim kodom (eng. *ransomware*) onesposobivši mogućnost poslovanja kako s korisnicima tako i s zaposlenima na tri dana. Šteta je procjenjena na 40 milijuna dolara koju su platili napadačima“ (Bloomberg, 2021.).[37]

[35] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet

[36] Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb, Ekonomski fakultet

[37] Bloomberg (2021.), CNA Financial Paid $40 Million in Ransom After March Cyberattack, preuzeto 7. rujna 2021. s https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

Rizik ometanja i provedbe transakcija, također, pripada skupini rizika provedbe poslovnih procesa. Ovaj rizik ima znatno veći opseg djelovanja od prije navedenog rizika neprekidnosti poslovanja, jer ne utječe na jednu instituciju i njihove klijente, već može imati posljedice za sve koji su uključeni u proces provedbe transakcija, poput platitelja, primatelja te institucije koje provode transakcije. „Upravo takva manifestacija rizika dogodila se prema The Seattle Times-u poduzeću AFTS iz Seattle-a, koje pruža usluge poput obrade plaćanja, naplatu, slanje poštom i druge usluge za općinska komunalna poduzeća i druge korisnike. Grupa hakera je putem zloćudnog koda (eng. *ransomware*) ukrala osjetljive podatke, uključujući financijske dokumente, prepisku sa zaposlenicima banke, kretanje računa, bilancu i porezne dokumente čija šteta još nije procijenjena“ (The Seattle Times, 2021.).[38] Drugoj najzastupljenijoj skupini rizika čija je značajnost naglo porasla u doba pandemije su infrastrukturni informatički rizici. Ovi rizici su posebno bitni za sva poduzeća koja su za vrijeme pandemije morala pronaći drugi način kako održavati timske sastanke te sastanke s klijentima, obzirom da se zbog epidemioloških mjera nisu mogli održavati uživo. Većina poduzeća takve sastanke zamijenila je virtualnim u točno unaprijed dogovoreno vrijeme. Dobar primjer nastupanja takvog rizika dogodio se nedavno. „Prema BBC-u napadnuta je informatička infrastruktura najvećeg informatičkog poduzeća na svijetu Microsoft-a te ujedno i jednog od njihovih najpoznatijih produkta – Microsoft Exchange servisa, jednog od najpoznatijih poslužitelja elektroničke pošte i kalendara. *Cyber* napad zahvatio je oko 250 tisuća servera ovog poslužitelja čime je u neposredni rizik otkrivanja povjerljivih informacija i podataka dovedeno oko 30 tisuća organizacija diljem svijeta“ (BBC, 2021).[39] Ovaj napad je jedan od najvećih napada zabilježenih u doba pandemije te dosta govori o tome koliko su i najveća i najnaprednija poduzeća ranjiva na ovakve ciljane hakerske napade.

[38] The Seattle Times (2021.), Hack of Seattle payments processing firm puts local governments on alert, preuzeto 7. rujna s https://www.seattletimes.com/seattle-news/hack-of-seattle-payments-processing-firm-puts-local-governments-on-alert/

[39] BBC (2021.), China accused of cyber-attack on Microsoft Exchange servers, preuzeto 7. rujna 2021. s https://www.bbc.com/news/world-asia-china-57889981

„U istraživanju provedenom od strane Engleskom Ministarstva za digitalizaciju, kulturu, medije i sport četiri od deset poduzeća (39 posto) i četvrtina dobrotvornih organizacija (26 posto) izvijestili su da su imali *cyber* napad u posljednjih 12 mjeseci. Kao i prethodnih godina, ovaj broj je veći među srednjim poduzeća (65 posto), velika poduzeća (64 posto) i dobrotvorne organizacije s visokim prihodima (51 posto)“ (Department for digital, culture, media & sport, 2021.).[40]

„Rizik od krađe povjerljivih osobnih podataka (eng. *phishing* napad) prema Carnetu podrazumijeva aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektroničke pošte i lažiranih web stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka kao što su korisnička imena i zaporke, PIN brojevi, brojevi kreditnih kartica i sl. U doba kada popularnost internet i mobilnog bankarstva i obavljanja transakcija putem interneta raste iz dana u dan, ovakvi napadi su posebno opasni i posebnu je pažnju potrebno posvetiti metodama njihovog sprječavanja“ (CARNeT, LS&S, 2005.).[41]

Upravo rizik od krađe povjerljivih osobnih podataka (eng. *phising*) u istraživanju Engleskog Ministarstva za digitalizaciju, kulturu, medije i sport je prikazano kao najčešći oblik napada u doba COVID-19 pandemije. „Od ukupnog broja ispitanih poduzeća između 79 i 83 posto odnosi se na *phising* napade“ (Department for digital, culture, media & sport , 2021.).[42] Takav rezultat ne čudi, obzirom da je takav oblik napada dosta teško prepoznati i često je jako uvjerljiv. „U Republici Hrvatskoj smo za vrijeme pandemije, također, imali razne primjere *phising* napada poput zlonamjernih poruka elektroničke pošte o kojem su obavijestili građane na svojim internetskim stranicama“ (ZSIS, 2020.).[43]

„Rizik od lažnog predstavljanja korištenjem socijalnog inženjeringa kako bi se došlo do financijskih podataka o poduzeću, je s 27 posto drugi po redu najzastupljeniji rizik od ukupnog broja ispitanih poduzeća prema istraživanju Engleskog Ministarstva za digitalizaciju, kulturu,

---

[40] Department for digital, culture, media & sport (2021.), Cyber security breaches survey 2021., preuzeto 6. rujna 2021. s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

[41] CARNeT, LS&S (2005.), Phising napadi, preuzeto 6. rujna 2021. s https://www.cis.hr/www.edicija/Phishingnapadi.html

[42] Department for digital, culture, media & sport (2021.), Cyber security breaches survey 2021., preuzeto 6. rujna 2021. s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

[43] Zavod za sigurnost informacijskih sustava, (2020.), Phising poruke elektroničke pošte [e-publikacija], preuzeto s https://www.zsis.hr/default.aspx?id=428

medije i sport“ (Department for digital, culture, media & sport, 2021.).[44] „Socijalni inženjering je postupak manipulacije osobama kako bi se izvele nedozvoljene akcije ili otkrile povjerljive informacije bez izravnog proboja u sustav. Izraz obično označava prikupljanje informacija, prijevaru ili dobivanje pristupa računalnom sustavu tako da se korisnike nagovori da predaju vjerodostojnice“ (CARNeT, 2006.). [45] „Rizik od neovlaštenog korištenja računala ili računalne mreže od strane zaposlenika treći s 15 posto od ukupnog broja ispitanih poduzeća prema istraživanju Engleskog Ministarstva za digitalizaciju, kulturu, medije i sport treći je najzastupljeniji. Važno je primijetiti da je u istom istraživanju na skoro četvrtom mjestu s oko 9 posto od ukupnog broja ispitanih poduzeća zlođudni virus (eng. *ransomware*)“ (Department for digital, culture, media & sport, 2021).[46]

Ovo istraživanje je samo pokazalo koji je oblik rizika bio najrašireniji i najuspješniji u Ujedinjenom Kraljevstvu u doba pandemije, obzirom da je većina *cyber* napada upravo bila usmjerena na pojedinca metodom socijalnog inženjeringa.

4.1.1 Analiza rizika internetskog i bezgotovinskog plaćanja

U doba COVID-19 pandemije, više nego ikada prije promovirano je bezgotovinsko plaćanja, misleći pritom ponajprije na beskontaktno plaćanje. Regulatorne agencije, banke i državne institucije internetsko i bezgotovinsko plaćanje okarakterizirale su kao sigurno, obzirom da se prilikom takvog provođenja transakcija ne uspostavlja fizički kontakt te se na taj način sprječava širenje virusa i posljedično zaraze. Na prvi pogled čini se kako se taj oblik plaćanja još više popularizirao i učinio sve raširenijim, dok je s druge strane takva promocija preko noći uzrokovala povećanje rizičnosti onih rizika kojima se u bližoj prošlosti nije pridavala velika značajnost.

Glavni rizici internetskih i bezgotovinskih plaćanja su zasigurno krađa osobnih podataka, od kojih su najznačajniji osjetljivi podaci popu PIN-a i broja računa na kartici koji omogućavaju da se transakcije provode na siguran način te ukoliko „padnu“ u ruke krive osobe mogu

[44] Department for digital, culture, media & sport (2021.), Cyber security breaches survey 2021., preuzeto 6. rujna 2021. s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

[45] CARneT (2006.) *Socijalni inženjering* [e-publikacija], preuzeto s https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-172.pdf

[46] Department for digital, culture, media & sport (2021.), Cyber security breaches survey 2021., preuzeto 6. rujna 2021. s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

prouzročiti velike novčane gubitke i rezultirati nepovjerenjem ljudi u takav oblik plaćanja. U doba pandemije često se događaju prijevare ovakvog karaktera. „Najbolji primjer takvih prijevara je veliki hakerski napad koje je rezultirao objavom na forum podatke o 10 000 tisuća korisnika American Express kartica sa sjedištem u Meksiku. Podaci su uključivali potpune brojeve kreditnih kartica i osobne podatke“ (CISOMAG, 2021.).[47] „Jedna od najznačajnijih oblika krađa podataka je *phising* oblik prijevare preko interneta koji se odnosi na socijalni inženjering poput lažnog predstavljanja putem elektroničke pošte ili napravljenih lažnih web stranica tako da izgledaju kao prava legitimna stranica nekog poduzeća. U tom slučaju ukoliko korisnik pri „lažnom“ plaćanju unese podatke poput PIN-a ili broja računa ili kartice, isti će se odmah prikazati onome tko je takvu prijevaru izradio. Ovakav oblik prijevare za vrijeme pandemije imao je Paypal, gdje su korisnici dobivali SMS poruke u kojima se tražilo da navedu svoje podatke od Paypal računa“ (Carnegie endowment for international peace, 2021.).[48]

Sve popularniji oblik plaćanja je elektroničko plaćanje putem digitalnog novčanika (eng. *e-wallet*) i mobilnih aplikacija poput Apple Pay-a, Google Pay-a ili Samsung Pay-a. Ovakav način plaćanja za sobom ostavlja pitanje sigurnosti samog uređaja i aplikacije kojom se izvršava plaćanje. „U istraživanju u Indiji istaknuta je činjenica kako je u Indiji u doba pandemije korištenje digitalnih novčanika poraslo za 44 posto te je dodatan razlog za zabrinutost sigurnosti plaćanja tim instrumentom sve veći broj korisnika koji u trenutku pisanja njihova rada iznosu više od 500 milijuna ljudi“ (Undale i sur., 2021.).[49] „Postoji iskrena zabrinutost da elektronički načini plaćanja mogu izložiti ljude i njihove podatke prijevari ili zlouporabi, osobito s aplikacijama za plaćanje. Telefoni se mogu hakirati te aplikacije mobilnog bankarstva nisu 100 posto sigurne. Zlonamjerne skupine iskoristile su krizu uzrokovanu pandemijom COVID-19 kako bi pojačale kibernetičke napade s većim brojem stanovništva koje radi od kuće, dok korisnici kupuju na nepoznatim web stranicama za e-trgovinu za kupnju robe i usluga. U travnju su *cyber* napadi poput krađe identiteta, lažnih web stranica ili izravnih napada bili tri puta veći od uobičajenih“ (Egerth, 2021.).[50]

---

[47] CISOMAG (2021.), Credit card data of 10,000 American Express accounts posted on Darknet Forum for free, preuzeto 10. rujna 2021. s https://cisomag.eccouncil.org/american-express-credit-card-data-sale-on-darknet/

[48] Carnegie endowment for international peace (2021.), Timeline of Cyber Incidents Involving Financial Institution, preuzeto 10. rujna 2021. s https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

[49] Undale, S., Kulkarni, A. and Patil, H. (2021.), Perceived eWallet security: impact of COVID-19 pandemic, *Vilakshan - XIMB Journal of Management*, Vol. 18 No. 1, pp. 89-104. https://doi.org/10.1108/XJM-07-2020-0022

[50] Egerth, K. (2021.), Cash is no longer king in times of COVID-19, preuzeto 7. rujna 2021. s https://www2.deloitte.com/ch/en/pages/consumer-industrial-products/articles/cash-is-no-longer-king-in-times-of-covid19.html

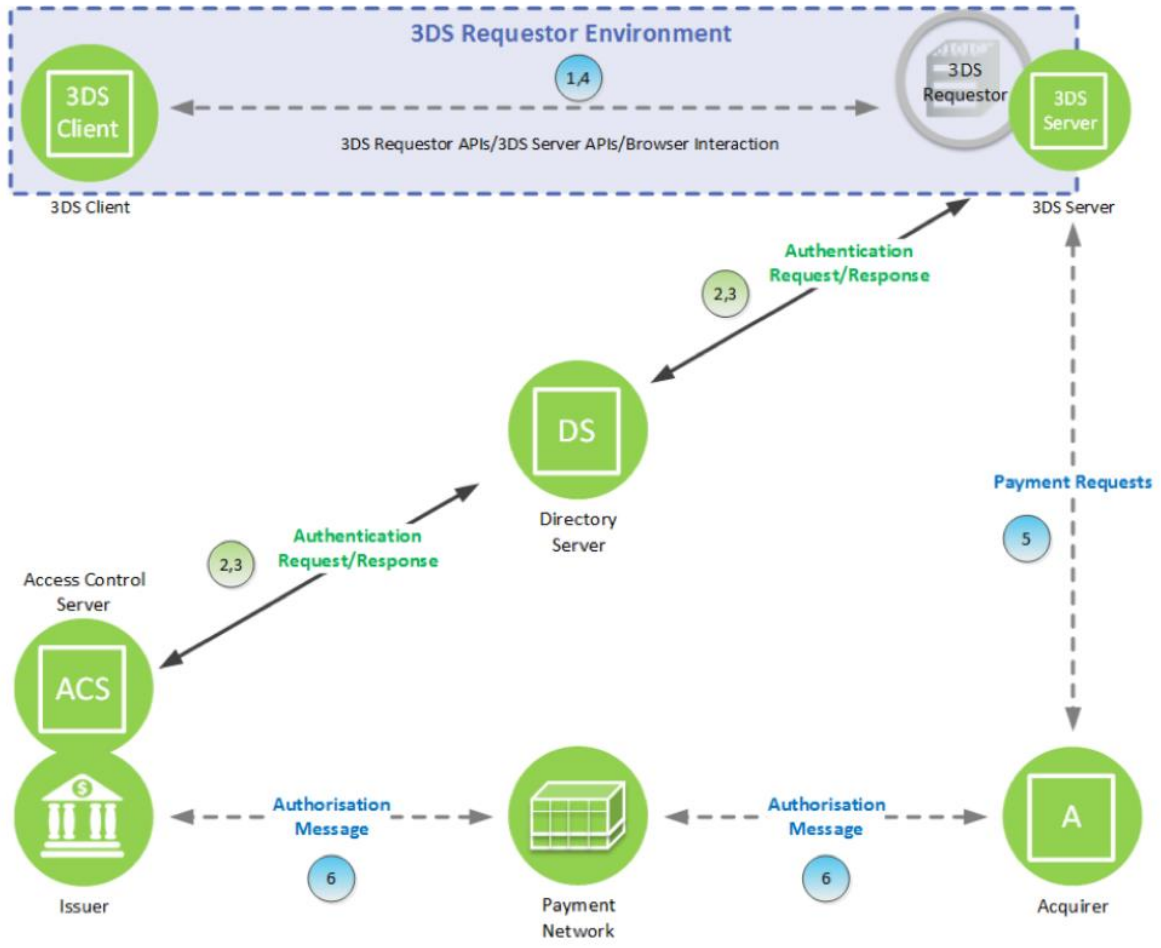
4.1.2 Zaštita internetskih i bezgotovinskih plaćanja

„Većina bezgotovinskih plaćanja provodi se putem neke vrste kartica poput: elektroničkih kartica, virtualne kartice pametne kartice i kartice lojalnosti, digitalnih novčanika, mobilna plaćanja, kartice s pohranjenom vrijednošću ili digitalna valuta“ (Bezhovski, 2016.).[51] Današnja metoda bezgotovinske naplate na prodajnim mjestima odvija se preko POS (eng. *Point of sale*) uređaja. POS terminali su uređaji koji na siguran i brz način omogućavaju plaćanja na mjestu prodaje i trenutan prijenos sredstva. Bezgotovinska plaćanja danas su jedan od najsigurnijih načina plaćanja, jer se pri prijenosu podataka koriste najsuvremenije metode poput P2PE (eng. *point to pint encryption*) kriptiranja podataka te su donesene brojne regulative i zakoni koji moraju biti zadovoljeni prije nego prodavaču bude dozvoljeno koristiti ovaj način provedbe transakcija. Kada se na POS terminalu plaća karticom ili beskontaktno karticom načinom zaštite plaćanja je provjera identiteta putem PIN-a, odnosno autentikacijske metode nečega što korisnik kartice zna svakih nekoliko transakcija, ili kada transakcija prelazi određen iznos kupnje. Slično vrijedi i za beskontaktno plaćanje mobilnim telefonom na POS terminalu, osim što je sada moguće potvrditi identitet i biometrijskom metodom otiska prsta, nešto što korisnik je – u ovom slučaju je to otisak prsta koji je jedinstven za svakog čovjeka. Internetska kupovina sve je više omiljen izbor kupnje za većinu ljudi. „Najbolje o tome govori podatak o sve većem postotku internetske kupovine u ukupnoj vrijednosti prodanih dobra. U doba pandemije taj udio se još više povećao o čemu najbolje govori provedeno istraživanje u kojem se navodi da je u nekim državama ta brojka u 2020. godini bila i 5 puta veća, nego u istom razdoblju 2019. godine. (McKinsey&Company, 2021.).[52] Prema tim podacima jasno je zašto je zaštita internetski transakcija izuzetno bitna. „Internetske transakcije zaštićene su *3-D Secure* protokolom kojeg je razvila EMVCo organizacija, a prihvatile su je sve velike kartične kuće na svijetu. EMVCo 3-D Secure (eng. *Three-domain secure protocol*) protokol je protokol za razmjenu poruka kako bi korisnicima omogućio autentikaciju kod svog izdavatelja kartice pri kupnji u e-trgovini bez kartice (eng. *card not present, CNP*). Dodatni sigurnosni sloj sprječava neovlaštene CNP transakcije i štiti trgovca od izloženosti CNP-a prijevari. Tri domene se sastoje od domene trgovca/stjecatelja, domene izdavatelja i domene interoperabilnosti“

[51] Bezhovski, Z. (2016.), The Future of the Mobile Payment as Electronic Payment System, European Journal od Business and Management, 8(8), 128.-129. str., https://core.ac.uk/download/pdf/234627158.pdf
[52] Lund, S., Madgavkar, A., Manyika, J., Smit,S., Ellingrud, K., Robinson O. (2021.), The future of work, after the COVID-19, preuzeto 10. rujna 2021., s https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19

(EMVCo, 2016.).[53] Protokol se temelji na procjeni rizičnosti kupnje na temelju navika korisnika, poput iznosa, uobičajenih internetskih trgovina ili ostalih parametara. Takav sustav napravljen je kako bi se minimizirali *man-in-the-middle* napadi te neovlaštena kupovina ukoliko netko pokuša tuđim identitetom provesti transakciju. Ovaj protokol predstavlja trenutno najveću razinu i vrhunac sigurnosti internetske kupovine te ga iz tog razloga koriste i najveće kartične kuće na svijetu poput *Vise, Mastercarda, American Expressa, Dinersa*. Ovaj sigurnosni protokol se koristi i prilikom internetske kupovine putem mobilnih telefona. Važno je napomenuti kako je 3-D Secure sustav usklađen s Revidiranom direktivom o platnim uslugama Europske unije, što je još jedan pokazatelj legitimnosti protokola.

Slika 1.: Izgled 3-D Secure protokola



Izvor: Modirum, 3-D Secure, dostupno na: https://www.modirum.com/3dsecure/

[53] EMVCo (2016.), EMV 3-D Secure, preuzeto 10. rujna 2021., s https://www.emvco.com/emv-technologies/3d-secure/

4.2 Primjer kvantifikacije *cyber* rizika

Kako bi bolje i jasnije shvatili utjecaj prijetnje te ozbiljnost nastupanja određenih *cyber* rizika, u ovom poglavlju bit će prikazan primjer nastupanja određenog rizika i njegov utjecaj na organizaciju prema Konceptu modela sistemskog rizika. „Sistemski rizik, definiran regulativom Europske unije je rizik od poremećaja u financijskom sustavu koji može imati ozbiljne negativne posljedice na unutarnje tržište i realno gospodarstvo“ (Europska komisija, 2010.).[54] „Konceptualni model dijeli analizu kibernetičkog incidenta u četiri različite faze: 1) kontekst, 2) šok 3) pojačanje i 4) sustavni događaj. Faze su temeljene na FSB-ovom (eng. *Financial stability board*) pristupu makro-financijskim implikacijama operativnog i kibernetičkog rizika, koji razlaže analizu kibernetičkog incidenta na opći kontekst incidenta, početni utjecajna izvora incidenta, njegovo pojačanje kroz sustav i konačni ishod. Faza konteksta opisuje okolnosti pod kojima dolazi do *cyber* incidenta, u oblik kristaliziranog kibernetičkog rizika. Ova faza ispituje sastavne dijelove kibernetičkog rizika koji predstavlja podrijetlo za potencijalni kibernetski incident, uključujući: *cyber* prijetnje, ranjivosti, imovinu, protumjere, početnu točku. Faza šoka opisuje neposredne tehničke i poslovne utjecaje do kojih je došlo na mjestu gdje incident ima svoj početni utjecaj. Faza pojačanja istražuje interakcije između zahvaćenih institucija i sustava koje koriste te čimbenike koji utječu na širenje šokova kroz te sustave. Faza sustavnog događaja ispituje točku u kojoj sustav više nije u stanju podnijeti *cyber* napad“ (ERSB, 2020.).[55]

Za primjer kvantifikacije rizika prikazat će se studija slučaja *cyber* napada na infrastrukturu izmišljene banke „X“ koja ima važnu ulogu u cjelokupnom platnom sustavu.

Primjer :

Banka ima značajnu ulogu u cjelokupnom platnom sustavu, pružajući infrastrukturu naplate manjim bankama na tržištu i ostalim institucijama u svojoj grupi. Za vrijeme ažuriranja softvera dogodio se *cyber* napad na softver za plaćanje i baze podataka banke X.

[54] Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010. on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board.

[55] ESRB (2020.) Systemic cyber risk, preuzeto 14. rujna 2021. s https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

Napad je trajao duži vremenski period, što je povećalo ozbiljnost problema nemogućnosti obavljanja osnovnih funkcija sustava te se novčana šteta počinje gomilati. Promatrajući ovaj *cyber* napad kroz Konceptualni model Sistemskog rizika možemo ga podijeliti u četiri različite faze: 1) kontekst 2) šok 3) pojačanje i 4) sistemskog događaj.

Faza konteksta: Incident se dogodio prilikom ažuriranja jednog od softvera za banke X, koji kontrolira plaćanje i sustav obrade. Taj softver održava treća strana dobavljač. Uoči redovnog noćnog izvođenja zakazane serije naloga za plaćanje, osoblje banke X pokušava ažurirati ključni dio softvera. Nakon primjene nadogradnje, tehničari počinju primjećivati nepravilnosti u radu sustava. Nakon naknadnog istraživanja postaje očito da je nadogradnja pošla po zlu te da se dogodio *cyber* napad.

Faza šoka: Sustav za obradu plaćanja već neko vrijeme ne radi ispravno, što rezultira milijunima transakcija koje se ne obrađuju. Incident dovodi do dugotrajne nedostupnosti računa salda u banci X. S obzirom na složenost procesa usklađivanja, postoje zabrinutosti o riziku integriteta podataka. Poslovne utjecaj očituje se u tome da je banka X suočena i prisiljena da privremeno ugasi sav promet procesuiranja transakcija. Iako je kratkoročni financijski utjecaj ograničen, dugoročni financijski, reputacijski i pravni utjecaji je mnogo veći

Faza pojačanja: Nedostupnost procesuiranja transakcija i stanja računa ima veliki učinak i zahvaća usluge koje banka X pruža svojim partnerima. Debitne kartice, kreditne kartice, aplikacije za internetsko i mobilno bankarstvo i gotovina neko vrijeme nisu dostupni. Incident je također utjecao na druga poduzeća unutar portfelja grupe Banke X, jer entiteti grupe dijele isto IT okruženje.

Faza sistemskog događaja: U ovom hipotetičkom scenariju, sve poslovne aktivnosti banke X ne rade. Internet i mobilno bankarstvo te fizički načine podizanja gotovine banke X nisu dostupni. Kupci nisu mogli pristupiti svom stanju na tekućem računu, izvršiti plaćanja i primati plaćanja kroz duži period. Unatoč stalnim naporima da odgovori na napad i oporavi se što brže, banka X je tek nakon što je prekinula poslovanje otkrila sigurnosni problem i sigurnosnom zakrpom riješila taj problem.

Dugotrajno ometanje značajnog dijela platnog sustava zemlje mogle bi izazvati velike razmjere financijska nestabilnost. U ovom primjeru, financijski gubitak zbog prekida poslovanja teško je procijeniti.

Uzmimo u obzir da je ovo samo financijski gubitak prekida poslovanja, dok su posljedice nastupanja reputacijskog i pravnog rizika puno veće i značajnije za budućnost poslovanja. Ovaj primjer dobro prikazuje koliki utjecaj jednog rizika male vjerojatnosti no velike značajnosti poput *cyber* napada na sustav za vrijeme njegove nadogradnje i namjerno zanemarivanje upravljanja sigurnosnim rizicima informacijskog sustava od strane menadžmenta može imati utjecaj na poslovanje jedne velike organizacije. Nastupanje jednog rizika često za sobom povlači i nastupanje drugih rizika koji u jednakoj ili većoj mjeri mogu imati utjecaj na cjelokupno organizaciju i budućnost njenog poslovanja, ako se rizicima aktivno ne upravlja.

4.3 Mjere zaštite regulatora i financijskih institucija

Početak 2020. godine zbog pojave pandemije bio je prilično neizvjestan, stoga su važne organizacije poput regulatora platnog prometa i financijskih institucija u Hrvatskoj, Europi i ostatku svijeta morali brzo donijeti važne odluke, smjernice i mjere kako bi se prije svega zaštitili ljudski životi te osiguralo neometano poslovanje usred privikavanja na „novo normalno“.

„Mjere Hrvatske narodne banke za ublažavanje ekonomskih posljedica pandemije dijele se na četiri cjeline: 1) Očuvanje kontinuiteta poslovanja ključnih funkcija HNB-a 2) Očuvanje kontinuiteta poslovanja kreditnih institucija 3) Mjere monetarne politike 4) Supervizorske mjere“ (HNB, 2020.).

„Očuvanje kontinuiteta poslovanja ključnih funkcija HNB-a prije svega se odnosi na očuvanje funkcija platnog prometa, trezorskog poslovanja (opskrba gotovinom), provedbe monetarne politike i upravljanja međunarodnim pričuvama i deviznom likvidnošću.

Za očuvanje kontinuiteta poslovanja kreditnih institucija HNB je zatražio od kreditnih institucija preispitivanje planova kontinuiteta poslovanja i planova upravljanja u kriznim situacijama, a osobito u dijelu: mjera za prevenciju širenja zaraze, osiguravanja tehnoloških i kadrovskih resursa za rad na daljinu, provedbe aktivnosti za neometano i sigurno funkcioniranje

IT sustava, provedbe aktivnosti za neometano funkcioniranje bankomatsko i EFTPOS mreže i sagledavanja potencijalnih negativnih rizika na kreditno poslovanje“ (HNB 2020.).[56]

„Mjere monetarne politike očituju se u stabilizaciji deviznog tečaja, osiguranja kunske likvidnosti i podupiranja stabilnosti tržišta državnih obveznica“ (ESRB, 2020.).[57]

„Supervizorske mjere očituju se u obustave određenih supervizorskih radnji, poput: nadzornog testiranja otpornosti na stres, neposredan nadzor poslovanja i ublažavanje dodatnih supervizorskih mjera“ (HNB, 2020.).[58]

„Mjere Hrvatske narodne banke vezane za financijske institucije koje imaju izravan utjecaj na fizičke osobe su sljedeće: u cilju minimiziranja kretanja i međusobnih kontakata, očekuje od banaka i kartičnih kuća da povećaju maksimalni iznos beskontaktne platne transakcije bez primjene pouzdane autentikacije klijenta (PIN) na 250 kuna. S ciljem smanjenja mogućnosti zaraze koronavirusom HNB je dao ovu preporuku jer će se navedenim iznosom obuhvatiti velik dio svakodnevnih platnih transakcija građana s obzirom na to da prosječna transakcija platnom karticom u Republici Hrvatskoj iznosi oko 225 kuna. Na razini kartičnog tržišta Republike Hrvatske, pojedinačni iznos beskontaktne elektroničke platne transakcije bez primjene pouzdane autentikacije klijenta ograničen je sada na 100 kuna, što je znatno manje od propisima maksimalno dopuštenih 50 eura (oko 370 kuna). Preporučena mjera osobito dolazi do izražaja ako se ima na umu da beskontaktne kartice u Republici Hrvatskoj čine većinu izdanih platnih kartica te su u obavljanju svakodnevnih transakcija iznimno zastupljene uz izuzetno dobru prihvaćenost kod korisnika i uz visoku razinu sigurnosti. Provođenje ove mjere bit će složen i tehnički zahtjevan proces koji uključuje različite dionike (izdavatelje platnih kartica, prihvatitelje platnih transakcija, pružatelje usluga procesuiranja platnih transakcija, kartične sheme) te zahtijeva međusobnu koordinaciju i suradnju. HNB očekuje da se navedena preporuka počne primjenjivati od strane svih dionika što je moguće prije, a zbog složenosti procesa najkasnije do 21. travnja 2020“ (HNB, 2020.).[59] „Hrvatska narodna banka, uzimajući

[56] HNB (2020.), *Mjere Hrvatske narodne banke za ublažavanje ekonomskih posljedica pandemije* [e-publikacija], preuzeto s https://www.hnb.hr/documents/20182/2953147/hn170320_prezentacija_Vujcic.pdf/bc719a93-ba7b-26ba-626e-950cf32dcf7f?t=1584467194434

[57] ESRB (2020.) Systemic cyber risk, preuzeto 14. rujna 2021. s https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

[58] HNB (2020.), Mjere Hrvatske narodne banke za ublažavanje ekonomskih posljedica pandemije, preuzeto 10. rujna 2021. s https://www.hnb.hr/documents/20182/2953147/hn170320_prezentacija_Vujcic.pdf/bc719a93-ba7b-26ba-626e-950cf32dcf7f?t=1584467194434

[59] HNB (2020.), HNB preporučuje povećanje maksimalnog iznosa beskontaktne platne transakcije bez primjene PIN-a sa 100 na 250 kuna, preuzeto 7. rujna 2021. s https://www.hnb.hr/-/hnb-preporucuje-povecanje-maksimalnog-iznosa-beskontaktne-platne-transakcije-bez-primjene-pin-a-sa-100-na-250-kuna

u obzir preporuke Stožera civilne zaštite Republike Hrvatske i Hrvatskog zavoda za javno zdravstvo u vezi s minimiziranjem kretanja i međusobnih kontakata, dala je preporuku bankama da privremeno ukinu naknadu fizičkim osobama za transakcije na bankomatima izvan vlastite mreže u Republici Hrvatskoj. Time se želi pridonijeti smanjenju rizika od zaraze jer se u tom slučaju građani ne bi koristili udaljenijim bankomatima svoje banke kako bi izbjegli dodane troškove, već bi mogli odabrati najbliži raspoloživi bankomat. HNB očekuje da se navedena preporuka počne primjenjivati što je moguće prije, a najkasnije od 25. ožujka 2020. te bude u primjeni u cijelom razdoblju trajanja ovih izvanrednih uvjeta izazvanih pojavom COVID-19. Također, bankama je upućena molba da razmotre mogućnost izdavanja debitnih kartica najugroženijim skupinama potrošača. To se ponajprije odnosi na starije osobe koje nemaju izdane debitne kartice po računima te na potrošače koji su zbog blokade otvorili zaštićene račune za koje neke banke nisu predvidjele izdavanje debitnih kartica.. Banke su pozvane i da razmotre mogućnosti kojima bi osigurale pristup poslovnicama s minimalnim rizikom zdravstvene ugroze za određene skupine građana (npr. izdvojeno vrijeme rada poslovnice za umirovljenike). Navedenim preporukama vodi se računa o najugroženijim kategorijama građana te onima kojima se preporučuje maksimalno ograničeno kretanje kako bi se njihova izloženost virusu COVID-19 svela na najmanju moguću mjeru“ (HNB, 2020.).[60]

„EBA (eng. *European banking authority*) poziva (2020.) nadležna tijela koja su odgovorna za nadzor kredita protiv AML/CFT i financijske institucije prema Direktivi (EU) 2015/8492 za potporu kreditnim i financijskim institucijama kontinuirani napori AML/CFT od strane da jasno stavi do znanja da je financijski kriminal neprihvatljiv, čak i u kriznim vremenima kao što je izbijanje epidemije: nastavak razmjene informacija o novim rizicima pranja novca i pranja novca i postavljanjem jasnih očekivanja korake koje bi kreditne i financijske institucije trebale poduzeti kako bi umanjile te rizike. Razmišljanje o tome kako privremeno prilagoditi uporabu svojih nadzornih alata kako bi se osiguralo kontinuirano sukladnost kreditnih i financijskih institucija s njihovim obvezama u pogledu AML/CFT“ (EBA, 2020.).[61]

Određena upozorenja i smjernice mogu se vidjeti i na internetskim stranicama organizacija za zaštitu nacionalnih informacijskih sustava, poput Hrvatskog Zavoda za zaštitu informacijskih

[60] HNB (2020.), HNB preporučuje privremeno ukidanje naknada za podizanje gotovine na bankomatima izvan vlastite bankomatske mreže, preuzeto 7. rujna 2021. s https://www.hnb.hr/-/hnb-preporucuje-privremeno-ukidanje-naknada-za-podizanje-gotovine-na-bankomatima-izvan-vlastite-bankomatske-mreze

[61] EBA (2020.), EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic, preuzeto 10. rujna 2021. s https://www.eba.europa.eu/eba-provides-additional-clarity-on-measures-mitigate-impact-covid-19-eu-banking-sector

sustava koji redovito izdaje upozorenja štetnim prijevarama fizičkih osoba. „Zavod za sigurnost informacijskih sustava je uočio novu *phishing* kampanju koja se širi putem elektroničke pošte. Radi se o poruci elektroničke pošte sa zlonamjernim privitkom u kojoj napadač kroz sadržaj naslova i poruke pokušava nagovoriti primatelja na otvaranje zlonamjernog privitka zavaravajući ga da se radi o obrascu putem kojeg se može doći do besplatne COVID-19 zaštitne opreme. U slučaju da korisnik otvori i pokrene zlonamjerni izvršni program iz privitka, program prikuplja podatke o lozinkama i prijavama koje korisnik ima na računalu te šalje rezultate prema poslužitelju **1**95.69.140.147 (port TCP 80) putem protokola HTTP. Radi se o inačici Lokibot zlonamjernog programa. U ovakvim slučajevima *phishing* napada koji uključuju zlonamjerne privitke ZSIS preporuča svojim korisnicima da prije otvaranja privitka provjere s pošiljateljem radi li se o legitimnom privitku, pogotovo ako se radi o elektroničkoj poruci koja dolazi izvan organizacije korisnika“ (ZSIS, 2020.).[62]

„U Sjedinjenim Američkim Državama, glavna regulatorna agencija FED (eng. *Federal Reserve System*) donijela je niz regulacija i supervizorskih mjera, kako bi na vrijeme zaštitila cjelokupnu ekonomiju i normalan rad platnog prometa. Mjere Federalnih rezervi kao odgovor na krizu COVID -19 može se grupirati u četiri kategorije. U prvoj kategoriji uključivale bi konvencionalne mjere monetarne politike poput smanjenja kamatnih stopa, ponude prosljeđivanje smjernica te ponovno povećanje i ponovno pokretanje programa za kupnju vrijednosnih papira Trezora i agencijske hipotekarne vrijednosne papire (MBS), kao i operacije repo ugovora. U drugu grupu uključene su mjere za osiguranje likvidnosti i financiranje za potporu novca funkcioniranje tržišta. U treću kategoriju uvrštene su brojne savezne ustanove. Pokrenute su rezerve za izravniju podršku protoku kredita kućanstvima, poduzećima i državi i lokalne uprave. U četvrtu skupinu uvrštene su privremene rekalibracije. Federalne rezerve donijele su propise i nadzornu praksu kako bi potaknule banke na podržavanje i protok kredita kućanstvima i poslovnim korisnicima“ (Clarida, Duygan-Bump i Scotti, 2021.).[63]

„Američka agencija za *cyber* sigurnost CISA uvidjela je problem sve češćih *cyber* napada na srednja i mala poduzeća te je shodno tome poduzela mjere svijesti i prevencije takvih napada. „Hakeri“, uključujući „hakere“ koje sponzorira država, sve više ciljaju pružatelje usluga upravljanja. Pružatelji usluga omogućuju daljinsko upravljanje informatičkim sustavima

[62] ZSIS (2020.), Upozorenje o phising kampanji na temu COVID-19, preuzeto 10. rujna 2021. s https://www.zsis.hr/default.aspx?ID=435

[63] Clarida, H., R., Duygan-Bump, B., Scotti, C. (2021.), The COVID-19 Crisis and the Federal Reserve's Policy Response., preuzeto 11. rujna 2021. s https://www.federalreserve.gov/econres/feds/files/2021035pap.pdf

korisnika i sustavima krajnjih korisnika. Veliki broj mala i srednja poduzeća koriste razne sustav pružatelja usluga za upravljanje IT sustavima, pohranu podataka ili podršku osjetljivim procesima. Pružatelji usluga obično korisnicima omogućuju proširenje i podršku mrežnih okruženja po nižoj cijeni nego što bi to učinili korisnici sami upravljati tim resursima. Pružatelji usluga općenito imaju izravan pristup mrežama i podacima svojih kupaca, što ih čini vrijednom metom kibernetičkih napada. „Hakeri" mogu iskoristiti odnose povjerenja poduzeća u mreže pružatelja usluga i dobiti pristup velikom broju klijenata. Ugrožavanje poslovanja malih i srednjih poduzeća mogu imati globalne učinke i uvesti značajan rizik poslovanja na tržištu. Iz tog razloga CISA je napisala sljedeće smjernice za zaštitu poslovanja. CISA preporučuje sljedeće smjernice za ublažavanje i pojačavanje zaštite: upravljanje rizicima u svojim sigurnosnim, pravnim i grupama za nabavu, pomoću procjena rizika identificirajte i odredite prioritete raspodjele resursa i kibernetička ulaganja, stvorite polaznu osnovu za ponašanje sustava i mreže radi otkrivanja budućih anomalija, neprestano nadgledajte sigurnosne informacije mrežnih uređaja i upozorenja uređaja za upravljanje događajima, redovito ažurirati softver i operativne sustave, upravljati rizicima autentikacije, autorizacije i računovodstvenih postupaka, pridržavati se najboljih praksi za upravljanje lozinkama i dopuštenjima, osigurati da računi pružatelja usluga nisu dodijeljeni administratorskim grupama i ograničiti te račune samo na sustave kojima upravljaju, odobriti pristup i administratorska dopuštenja na temelju potreba za znanjem i najmanjih privilegija, provjerite koriste li se računi davatelja usluga u odgovarajuće svrhe i onemogućeni su kada se ne koriste aktivno" (CISA, 2021.).[64]

Možemo reći kako su se regulatorne agencije brzo reagirale kako se postupno pogoršavala situacija s COVID-19 pandemijom u svijetu. U ovoj pandemiji se najbolje vidjelo koliko su važni svjetski regulatori dobro umreženi te brzini prepoznavanja rizika kada se radi o globalnom problemu. „I ostale financijske institucije poput banaka isto su dobro reagirale implementirajući sve važne preporuke i odluke koji su ima regulatori savjetovali ili propisali poput povećanja limita beskontaktnih plaćanja bez provjere identiteta ili naknada za podizanje gotovine na bankomatima izvan vlastite bankomatske mreže" (HNB, 2020.).[65] Ovakav scenarij bio je očekivan, obzirom da su se brojne regulative promijenile od 2008. godine kada je nastala

[64] CISA (2021.), Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses, preuzeto 10. rujna 2021. s https://www.cisa.gov/sites/default/files/publications/CISA%20Insights_Guidance-for-MSPs-and-Small-and-Mid-sized-Businesses_S508C.pdf

[65] HNB (2020.), HNB preporučuje privremeno ukidanje naknada za podizanje gotovine na bankomatima izvan vlastite bankomatske mreže, preuzeto 10. rujna 2021. s https://www.hnb.hr/-/hnb-preporucuje-privremeno-ukidanje-naknada-za-podizanje-gotovine-na-bankomatima-izvan-vlastite-bankomatske-mreze

zadnja velika financijska kriza, poput povećanja stope obvezne rezerve, što je uvelike poboljšalo otpornost i spremnost financijskih institucija na ovakve neočekivane stresove.

5. Istraživanje percepcije sigurnosti bezgotovinskih plaćanja

U svrhu istraživanja Percepcije korisnika o zaštiti bezgotovinskih plaćanja u doba COVID-19 pandemije provedena je anketa putem interneta. Za potrebe provođenja ankete izrađen je anketni upitnik pomoću Google-ove aplikacije Google Forms.

5.1 Opis istraživanja

Istraživanje Percepcije korisnika o zaštiti bezgotovinskih plaćanja u doba COVID-19 pandemije provedeno je u razdoblju od 12. do 19. srpnja 2021. godine. Istraživanje je primarno provedeno putem interneta preko društvene mreže Facebook te je u istraživanju je sudjelovalo ukupno 330 ispitanika koji su anketni upitnik ispunili do kraja, različitih dobnih skupina te ostalih demografskih obilježja. Društvena mreža Facebook odabrana je kao primaran način sakupljanja podataka obzirom da se na toj društvenoj mreži anketa može provesti na brz način i pritom postići najveći doseg kod ljudi različite dobi, spola i ostalih demografski obilježja. Nakon pronalaska i analize ostalih provedenih istraživanja, u kojima su se uzorci ispitanika kretali između 150 i 250 ispitanika, zaključeno je kako bi veća brojka ispitanika u istraživanju prikazala preciznije rezultate, tim više što je COVID-19 pandemija zahvatila sve dobne skupine koje su u određeno doba pandemije bili primorani ponašati se na isti način, poput korištenja internetske kupovine te bezgotovinskih transakcija za određenu skupinu proizvoda, obzirom da je većina fizičkih trgovina bila zatvorena. Uzorak od 330 ispitanika raznih demografskih obilježja dovoljno je velik i relevantan, kako bi se iz njega mogli izvesti svi zaključci potrebni za ovo istraživanje.

5.2 Ciljevi istraživanja

Osnovni cilj istraživanja je prikazati i diskutirati rezultate, usporediti ih s ostalim tematski sličnim istraživanjima, te dodatno objasniti i analizirati rezultate. Prikupljeni rezultati bit će analizirani i diskutirani te uspoređeni sa sličnim istraživanjima na način da se usporede podaci iz razdoblja prije pandemije i razdoblja u pandemiji, kako bi se potvrdile sličnosti trenda i moguća odstupanja.

Rezultati istraživanja dati će odgovor na pitanje jesu li, i u kojoj mjeri u donesene upute i mjere zaštite od strane regulatora i financijskih institucija utjecale na rizike sigurnosti i zaštite platnog prometa u doba pandemije.

5.3 Metodologija istraživanja

Za metodologiju istraživanja odabrana je metoda prikupljanja primarnih podataka putem anketnog upitnika. U svrhu istraživanja izrađen je anketni upitnik koji se sastoji od tri dijela i ukupno 42 pitanja. Anketa se sastoji od dvije vrste pitanja: pitanja s višestrukim odabirom odgovora te Likertove ljestvice od 5 stupnjeva za mjerenje stavova u kojoj su sudionici morali odabrati u kojoj mjeri se slažu s određenom tvrdnjom. Sva pitanja za anketni upitnik su strukturirana u skladu s potrebama i ciljevima istraživanja. Prvi dio upitnika sastoji se od 8 pitanja koja se odnose na razdoblje prije COVID-19 pandemije, u drugom dijelu postavljena su 12 pitanja koja se odnose na razdoblje u doba COVID-19 pandemiji. Treći dio upitnika sastoji se od 4 pitanja koja se odnose na demografska obilježja ispitanika kako bi bolje mogli napraviti analizu rezultata te potvrditi reprezentativnost uzorka. Anketna pitanja napravljena su i prilagođena za ovu temu na temelju pitanja u sličnim istraživanjima, kako bi se dobiveni rezultati mogli lakše usporediti i dodatno objasniti. Istraživanja putem ankete koje su provedene doba pandemije i bave se sličnom tematikom su „anketna istraživanja Odjela za digitalizaciju, kulturu, medije i sport Ujedinjenog Kraljevstva“ (Department for digital, culture, media & sport, 2021.) [66] o cyber sigurnosti u 2020. i 2021. godini i Deloitte-ovo „istraživanje o utjecaju COVID-19 pandemije na financijsku industriju i platni promet“ (Deloitte, 2020.).[67] Istraživanje zaštite bezgotovinskih transakcija je provedeno putem interneta preko društvene mreže Facebook, obzirom da se na toj društvenoj mreži anketa može provesti na najbrži način i postići najveći doseg kod ljudi različite dobi, spola i ostalih demografski obilježja. Anketni upitnik je u potpunost dobrovoljan, anoniman te namijenjen svim osobama bez obzir na njihovu dob, spol itd. Rezultati dobiveni ovim istraživanjem korišteni su isključivo u svrhu pisanja ovog diplomskog rada. Na temelju prikupljenih podataka napravljena je analiza rezultata prikazana u potpoglavlju Analiza rezultata istraživanja.

[66] Department for digital, culture, media & sport (2021.), Cyber security breaches survey 2021., preuzeto 6. rujna 2021. s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

[67] Deloitte (2020.), European COVID-19 survey, preuzeto 6. rujna 2021. s https://www2.deloitte.com/content/dam/Deloitte/it/Documents/financial-services/Deloitte_COVID%20Survey%20on%20Payment%20Services_IV2020.pdf

Prikaz dizajna pitanja iz ostalih istraživanja na temelju kojeg je dizajnirano istraživanje percepcije korisnika o zaštiti bezgotovinskih transakcija. Pitanja iz ovih istraživanja služila su kao navigacijski okvir za usporedbu rezultata prije i u doba pandemije.

Tablica 1.: Primjer pitanja iz istraživanja Odjela za digitalizaciju, kulturu, medije i sport Ujedinjenog Kraljevstva

Pitanje	Ponuđeni odgovori
1. Kakva je razine percepcija *cyber* sigurnosti vaše organizacije?	a) Vrlo visoka b) Visoka c) Vrlo niska d) Niska
2. Koliko ste *cyber* napada imali u zadnjih 12 mjeseci?	a) niti jedan b) 1-2 napada c) 3-5 napada d) Više od 5
3. Jeste li u odnosu na 2020. primijetili manje *cyber* napada?	a) Da b) Ne c) Ne mogu odrediti

Tablica 2.: Primjer pitanja iz istraživanja Deloitte-a o utjecaju COVID-19 pandemije na financijsku industriju i platni promet

Pitanje	Ponuđeni odgovor
1. U usporedbi s razdobljem prije pandemije COVID-19, u kojoj mjeri će se vratit korištenje gotovine u plaćanjima?	a) Da b) Ne
2. Jeste li tijekom pandemije iskusili bilo kakav operacijski incident?	a) bez incidenata b) manji incidenti c) veliki incidenti
3. Je li pandemije utjecala na planove vaše organizacije?	a) Da b) Ne
4. Na što banke stavljaju svoj fokus?	a) Na digitalno bankarstvo b) otvoreno bankarstvo c) SMB d) Instant transakcije

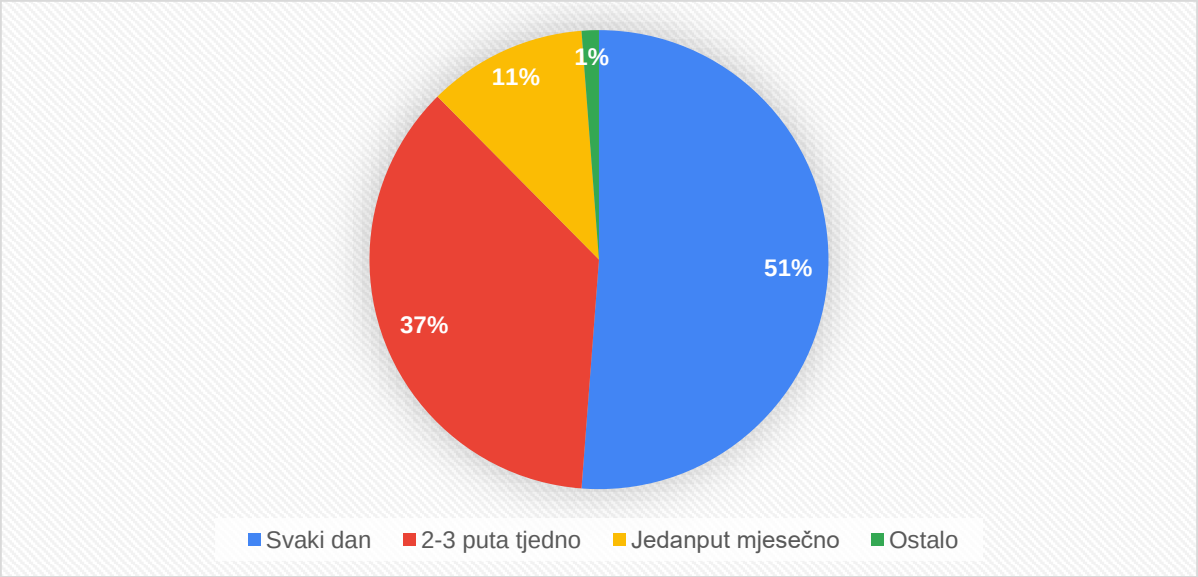
5.4 Uzorak ispitanika

Uzorak ispitanika sastoji se od ljudi različitih demografskih obilježja, od kojih su za ovo istraživanje najbitnija: dob, spol, dohodak, razina obrazovanja i status zaposlenosti ispitanika. Navedena demografska obilježja jamče reprezentativnost uzorka te se različitost uzorka može vidjeti u poglavlju analiza rezultata (grafovi: 21, 22, 23 i 21). Anketa je bila osmišljena na način da bude razumljiva svim dobnim skupinama, kako bi je moglo ispuniti što više ljudi različite dobi. Veličina uzorka od 330 ispitanika, još je jedan pokazatelj reprezentativnosti uzorka, obzirom da broj ispitanika uvelike utječe na rezultate i krajnji ishod ankete.

5.5 Analiza rezultata istraživanja

U provedenom istraživanju ukupno je 330 ispitanika ispunilo anketni upitnik te su u nastavku prikazani dobiveni rezultati. Rezultati istraživanja su detaljno deskriptivno analizirani i grafički prikazani, kako bi se u uzorku mogla lakše prikazati raspodjela odgovora.

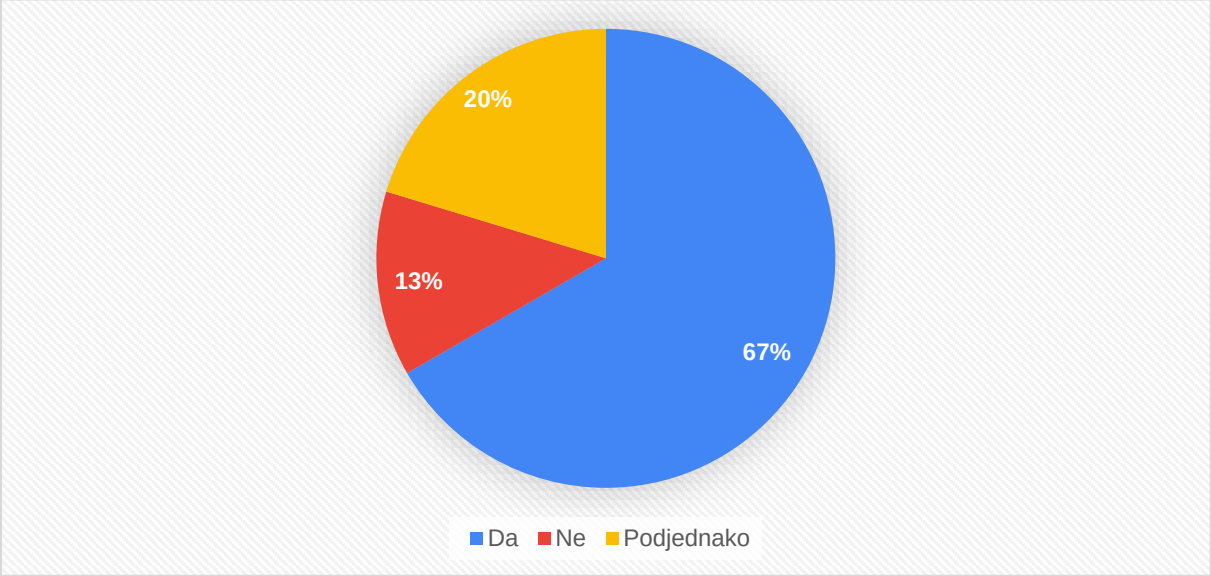
Grafikon 1.: Učestalost bezgotovinskih transakcija u kupovini



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Prilikom kupovine najviše ispitanika se koristi bezgotovinskim financijskim instrumentima, njih 87,6 posto, dok ostatak ispitanika bezgotovinska plaćanja koristi samo jedanput mjesečno do nekoliko puta godišnje. Manji dio uzorka, tek 1,2 posto, ne koristi bezgotovinske instrumente te je odabralo isključivo gotovinsko plaćanje.

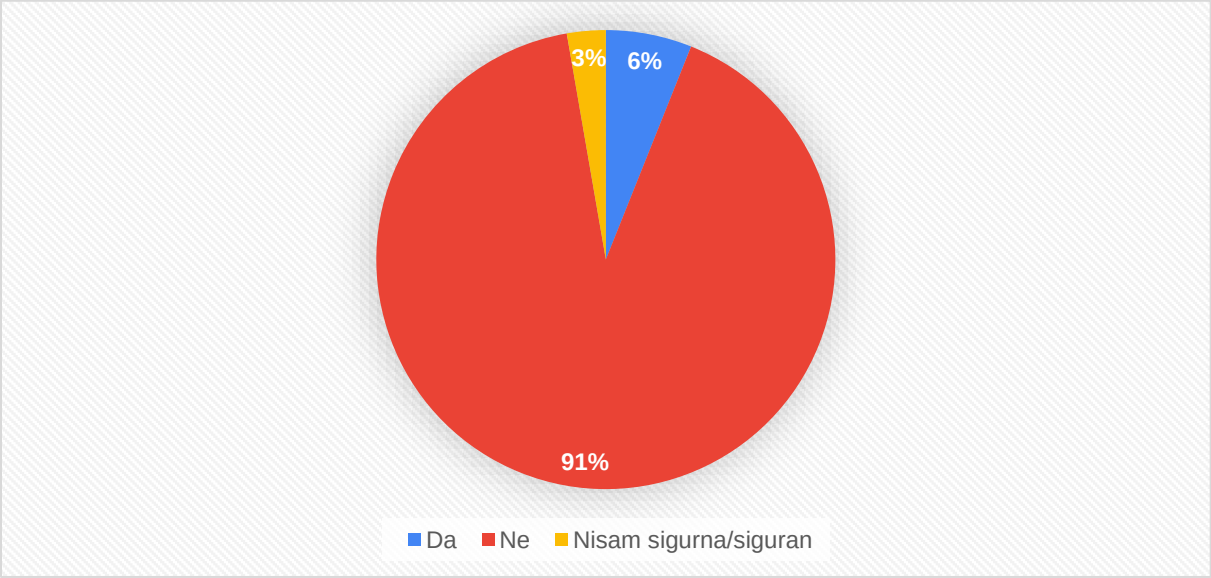
Grafikon 2.: Preferencije bezgotovinskih transakcija i internetske kupovine



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Većina ispitanika preferira internetsku kupovinu i bezgotovinska plaćanja, njih 66,7 posto, dok ostatak uzorka od 20,3 posto kaže da preferiraju podjednako u odnosu na fizičke prodajna mjesta i gotovinsko plaćanje. Manji dio ispitanika ne preferira internetsku kupovinu i bezgotovinska plaćanja, njih 13 posto.

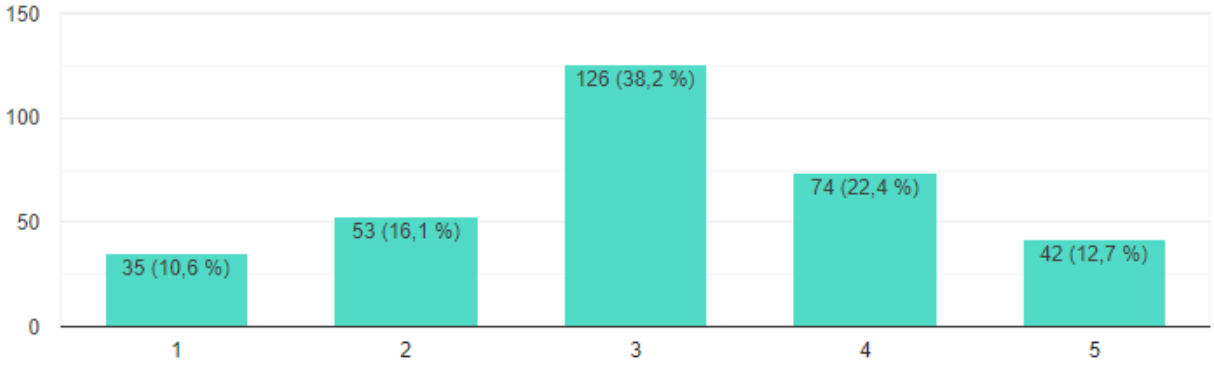
Grafikon 3.: Ispitanici koji su bili žrtve prijevare bezgotovinske transakcije prije COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Većina ispitanika nije nikada bilo žrtva prijevare bezgotovinskog načina plaćanja, njih 91,2 posto, dok je manji dio bio ili nije siguran. Iako je tek manji dio bio prevaren ili nije siguran, 8,8 posto je veliki postotak ukoliko se prijevara stvarno dogodila ili se na nju sumnja.

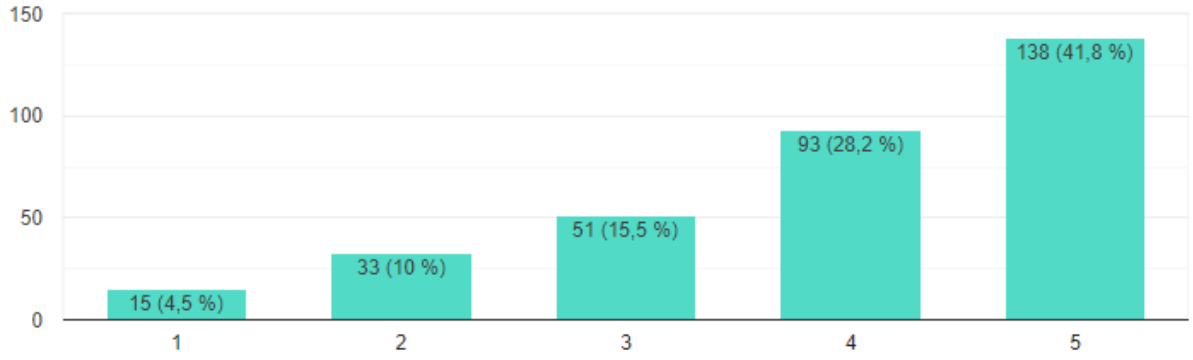
Grafikon 4.: Preferencija ispitanika o bezgotovinskim plaćanjima i internetskoj kupovini



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

U ovom primjeru može se vidjeti trend gdje većina ispitanika nije sigurna u sigurnost podataka prilikom bezgotovinskih transakcija i internetske kupovine, dok je druga najzastupljenija skupina ipak korisnici koji vjeruju da su podaci sigurni. Iako najmanje zastupljena skupina, velik dio ispitanika misli da podaci nisu sigurni ili u potpunosti sigurni prilikom bezgotovinskih transakcija i internetske kupovine, njih 26,7 posto.

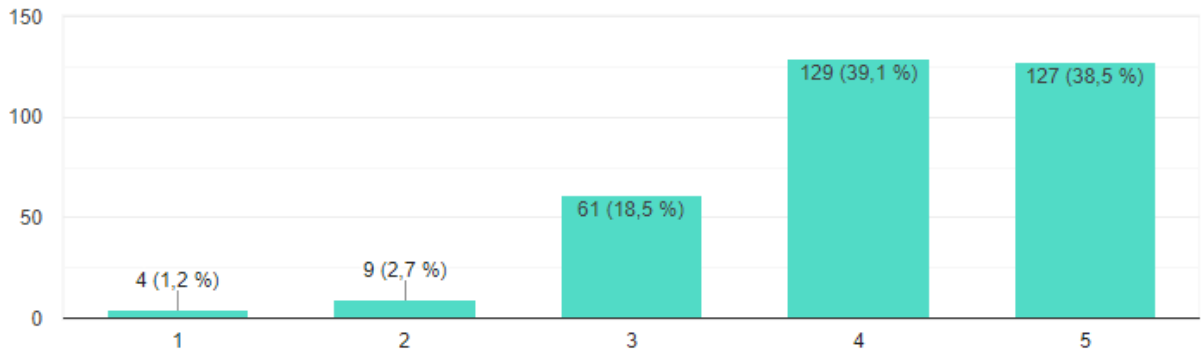
Grafikon 5.: Broj ispitanika koji je i prije COVID-19 pandemije često koristio bezgotovinska sredstva plaćanja



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Prije COVID-19 pandemije 70 posto ispitanika je koristilo bezgotovinska sredstva plaćanja, dok je 15 posto koristilo gotovinu kao primarno sredstvo plaćanja, a njih 15 posto su u jednakoj mjeri koristili gotovinu i bezgotovinska sredstva plaćanja.

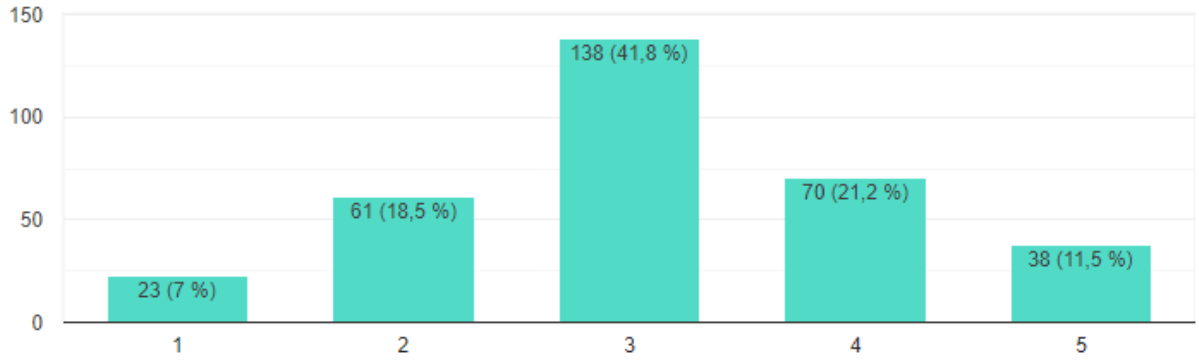
Grafikon 6.: Percepcija korisnika o pouzdanosti bezgotovinskog plaćanja



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Ukoliko promatramo stupce 4 i 5 zajedno, većina ispitanika smatra, njih 60,4 kako je bezgotovinsko plaćanja pouzdano, te stupci 3, 2 i 1 skupno promatrano 21,9 misli da bezgotovinsko plaćanje još uvijek nije sigurno. Njih 18,5 nisu sigurno u ovu tvrdnju.

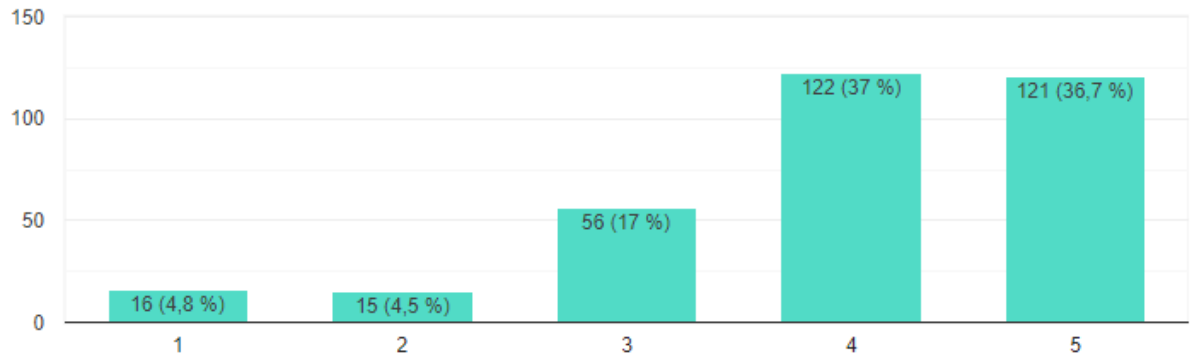
Grafikon 7.: Percepcija ispitanika o učestalosti internetskih prijevara prije COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

U ovom primjeru možemo vidjeti kako većina ispitanika ipak nije sigurna je li u doba prije pandemije bilo više internetskih prijevara, dok 32,7 posto misli da ih je bilo manje. Samo mali broj uzorka misli da ih u doba pandemije nije bilo više, njih 25,5 posto.

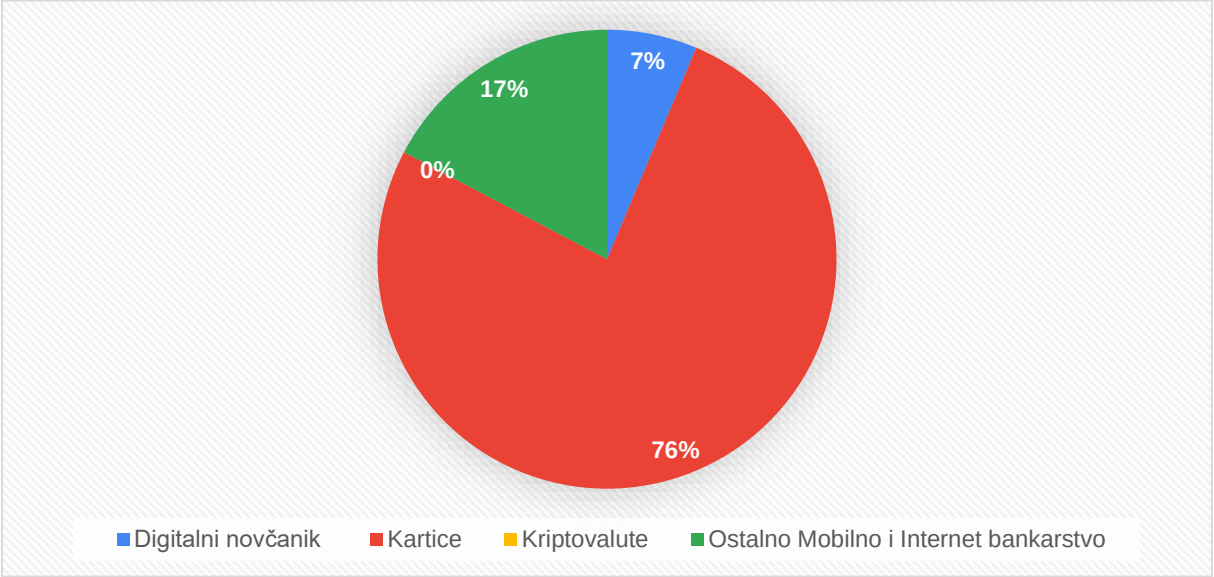
Grafikon 8.: Broj ispitanika koji će i nakon pandemije primarno nastaviti koristiti bezgotovinska sredstva te kupovati preko interneta zbog zadovoljstva razine sigurnosti



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Nakon pandemije će 73,7 posto ispitanika primarno nastaviti koristiti bezgotovinska sredstva te kupovati preko, dok će manji dio od tek 9,3 posto nastaviti plaćati tradicionalnim sredstvima. Manji dio ispitanika, njih 17 posto nije sigurno.

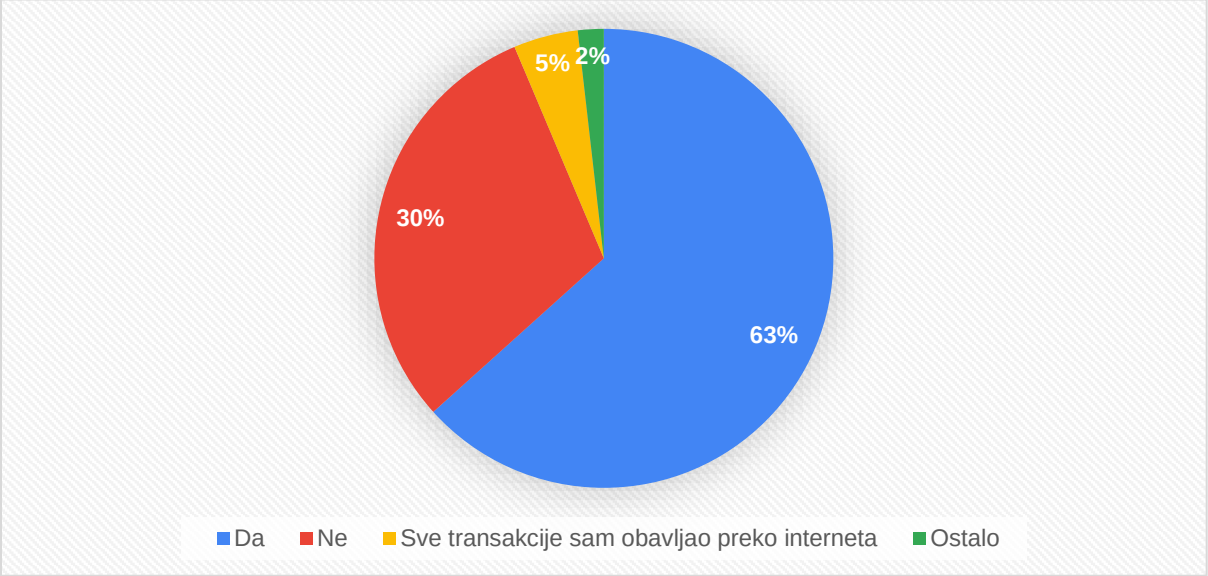
Grafikon 9.: Prikaz preferiranog oblika bezgotovinskog plaćanja za vrijeme COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Većina ispitanika, njih 76,4 posto odabralo je kartice kao preferirani oblik plaćanja, dok je drugo najzastupljenije mobilno i Internet bankarstvo s 17,3 posto. Od ostatka ispitanika, njih 21 posto preferira koristiti digitalni novčanik poput Google i Apple pay-a. Zanimljivo je da u doba pandemije nitko od ispitanika nije odabrao plaćanje kriptovalutama kao preferirano.

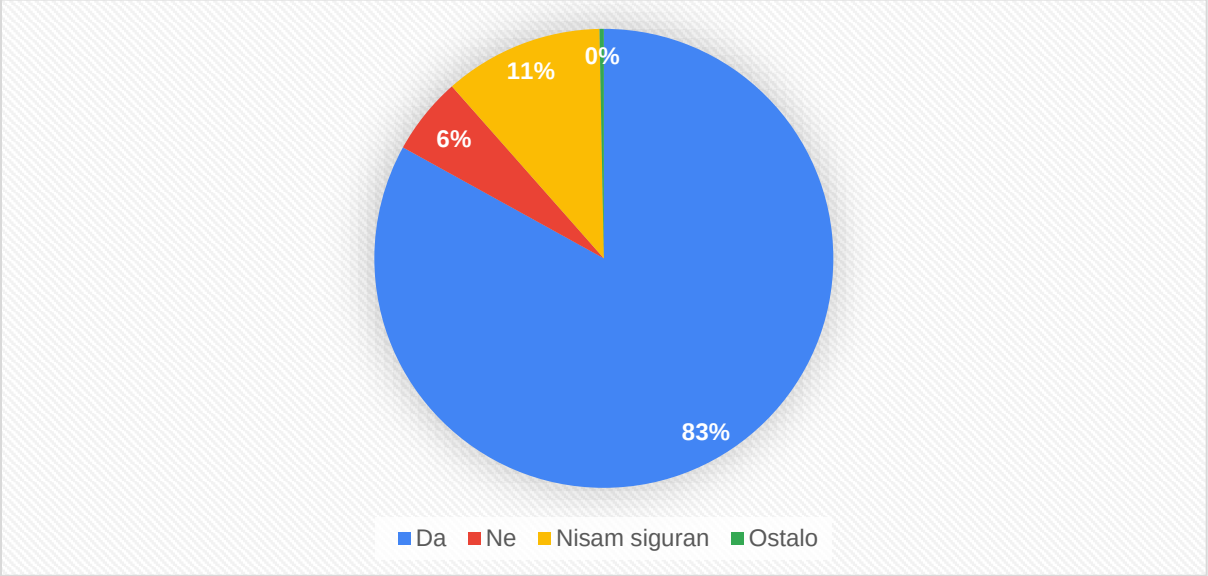
Grafikon 10.: Prikaz kupovine preko interneta u doba COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Ispitanici su većinski odgovorili da su za vrijeme pandemije preko interneta kupovali više, nego prije, dok je 30 posto odgovorilo kako nisu kupovali više za vrijeme pandemije. Manji dio uzorka od 4,5 posto odgovorio je kako su svu kupovinu obavljali putem interneta.

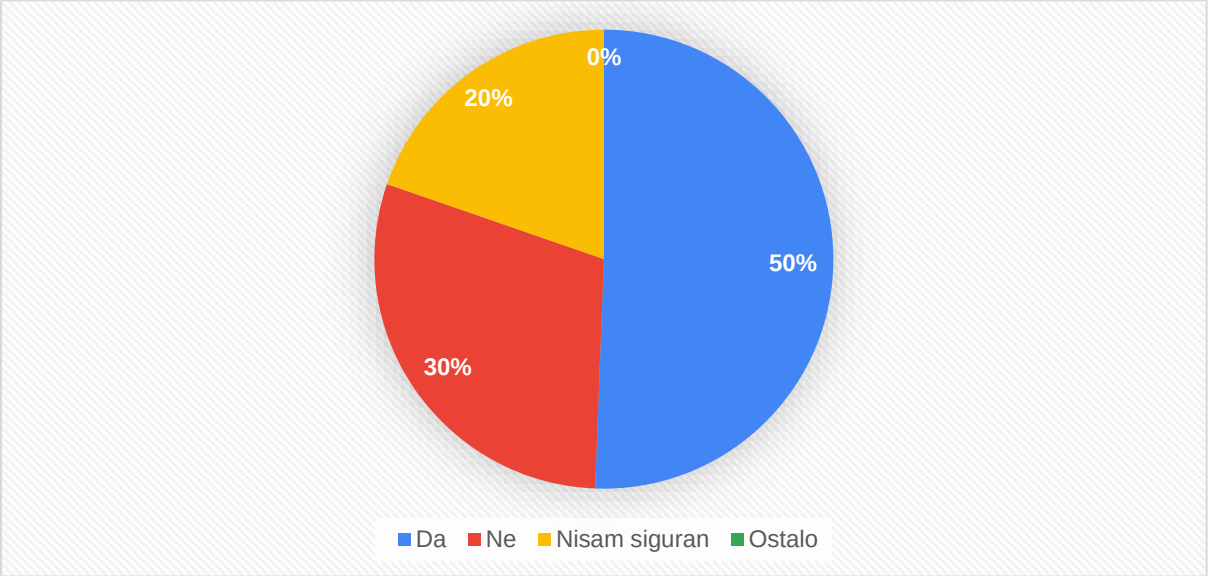
Grafikon 11.: Prikaz pokušaja prevare prilikom internetskog ili drugog bezgotovinskog plaćanja



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Ispitanici su većinski odgovorili kako nisu bili žrtve pokušaja prijevare, dok s druge strane njih 16,7 posto tvrdi kako su ili bili žrtva pokušaja prijevare ili nisu sigurni tj. ne znaju jesu li prepoznali prijevaru.

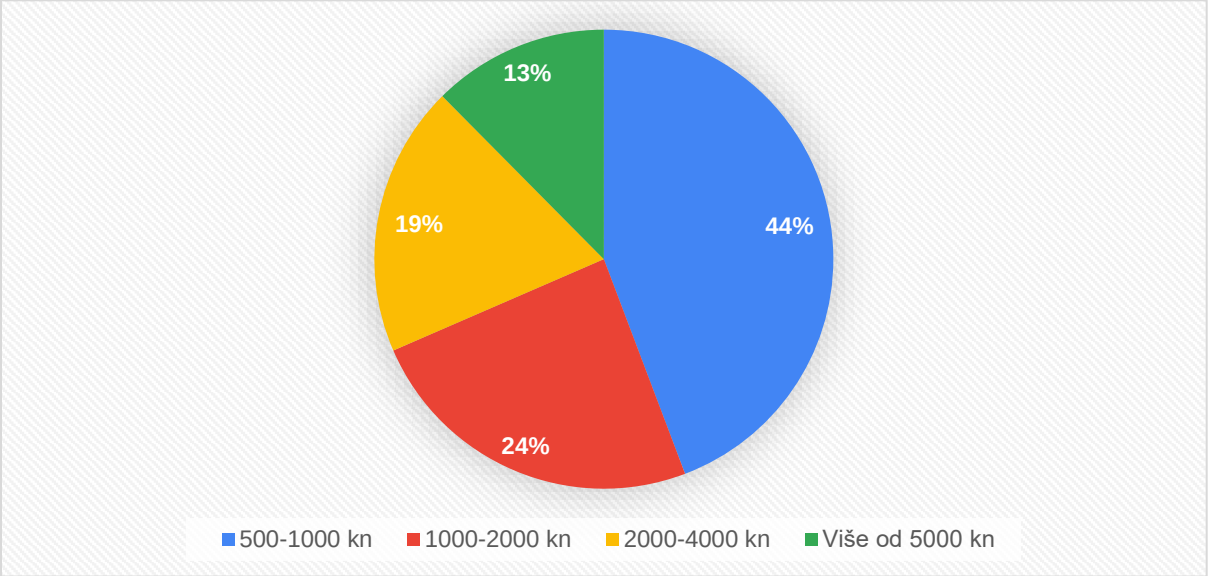
Grafikon 12.: Prikaz učestalosti zahtjeva za autentikacijom od strane banke prilikom internetskog ili bezgotovinskog plaćanja tijekom COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Više od pola ispitanika je odgovorilo da su bili traženi da se češće autenticiranju prilikom plaćanja u doba pandemije, čak 50,6. Manji dio s 29,7 posto je odgovorilo da nisu bili traženi da se češće autenticiraju. Tek manji dio, 19,7 je odgovorio da nisu sigurni.

Grafikon 13.: Prikaz najveće bezgotovinske transakcije koju su ispitanici napravili u doba COVID-19 pandemije

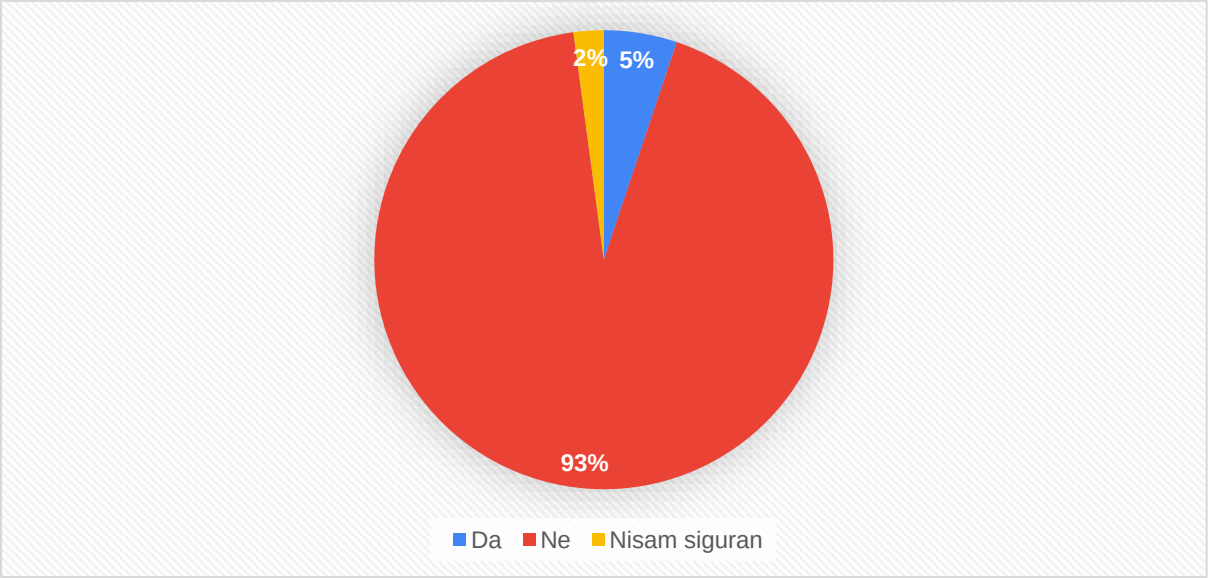


Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Najveći dio ispitanika, njih 44,2 posto, odgovorio je da su im najveće transakcije u doba pandemije iznosile između 500 – 1000 kuna. Njih 24,2 posto odgovorilo je da im je najveća

transakcija u doba pandemije iznosila između 1000 – 2000 kuna. Dio ispitanika od 19,1 posto odgovorilo je kako im je najveća transakcija u doba pandemije iznosila između 2000 – 4000 kuna, dok je najmanji dio od 12,4 posto odgovorio da im je najveća transakcija iznosila više od 5000 kuna.

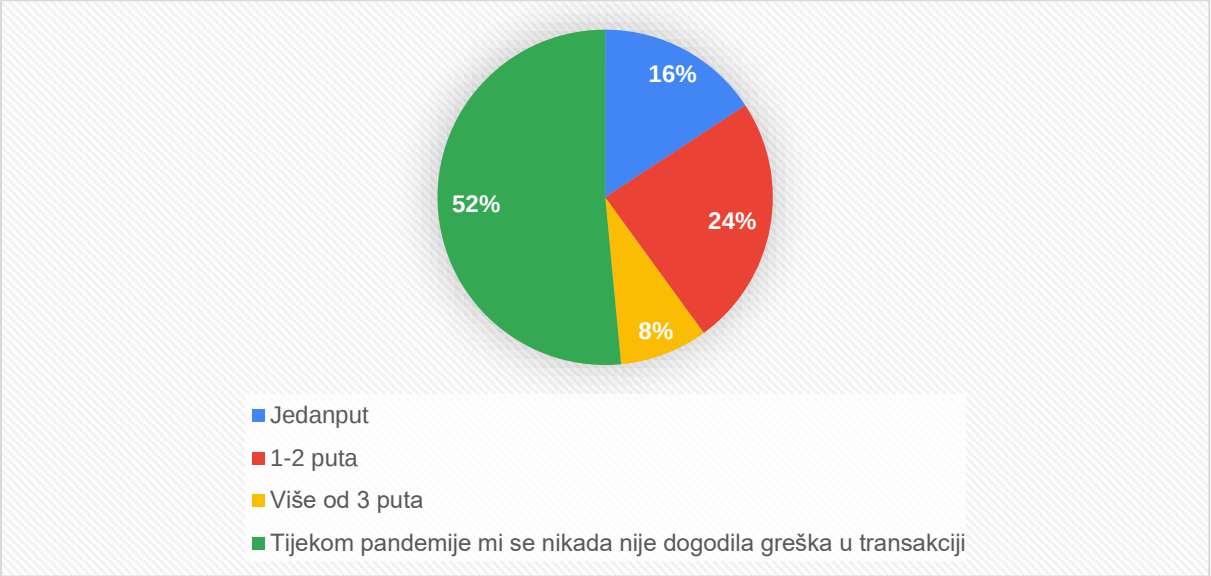
Grafikon 14.: Prikaz odbijanja transakcija prilikom plaćanja od strane banke u doba COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Većina ispitanika, njih 92,7 posto odgovorilo je kako im banka nije odbila bezgotovinsku transakciju u doba pandemije, dok njih 7,3 tvrdi kako im je banka odbila transakciju ili nisu sigurni.

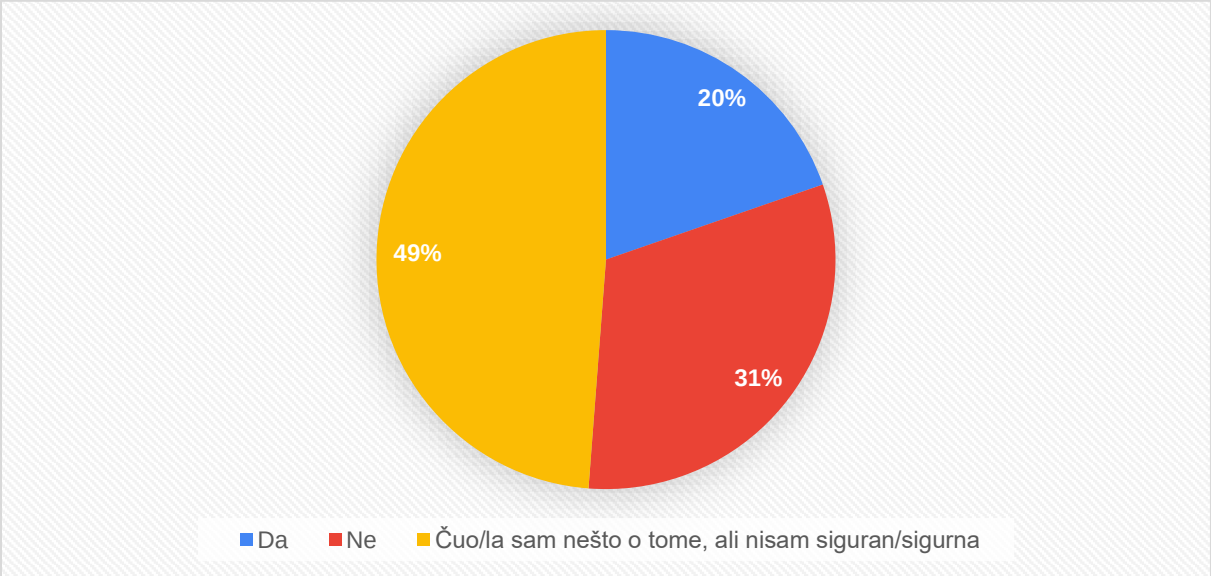
Grafikon 15.: Prikaz učestalosti nastanka pogreške prilikom plaćanja zbog koje ispitanici nisu mogli izvršiti transakciju



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

S 51,5 posto ispitanika, više od polovice je odgovorilo da im se tijekom pandemije nikada dogodila greška zbog koje nisu mogli završiti transakciju. S druge strane 48,5 posto odgovorilo je da im se tijekom pandemije dogodila barem jednom dogodila greška zbog koje transakciju nisu mogli izvršiti do kraja. Od 48,5 posto, čak 32,7 posto ispitanika se takva greška dogodila jedan do dva ili više od tri puta.

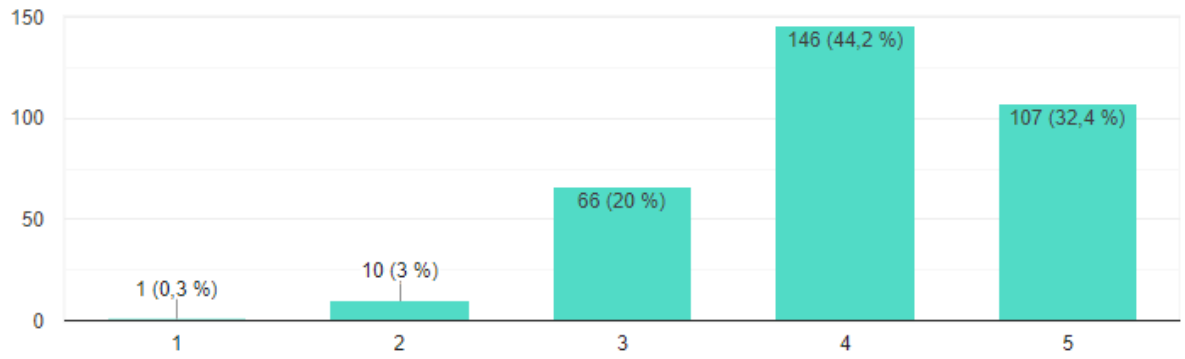
Grafikon 16.: Prikaz upoznatosti ispitanika sa smjernicama i odlukama o sprječavanju prijevara prilikom bezgotovinskih i internetskih plaćanja u doba COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Ispitanici su većinski s 48,8 posto odgovorili kako nisu bili upoznati s sa smjenricama i odlukama o sprječavanju prijevara prilikom bezgotovinskih i internetskih plaćanja u doba COVID-19 pandemije, dok je njih 31,5 posto odgovorilo da su je čulo nešto o tome, ali s time nisu upoznati. Samo je 19,7 ispitanika odgovorilo kako je čulo za smjernice i odluke o sprječavanju prijevara prilikom bezgotovinskih i internetskih plaćanja u doba COVID-19 pandemije.

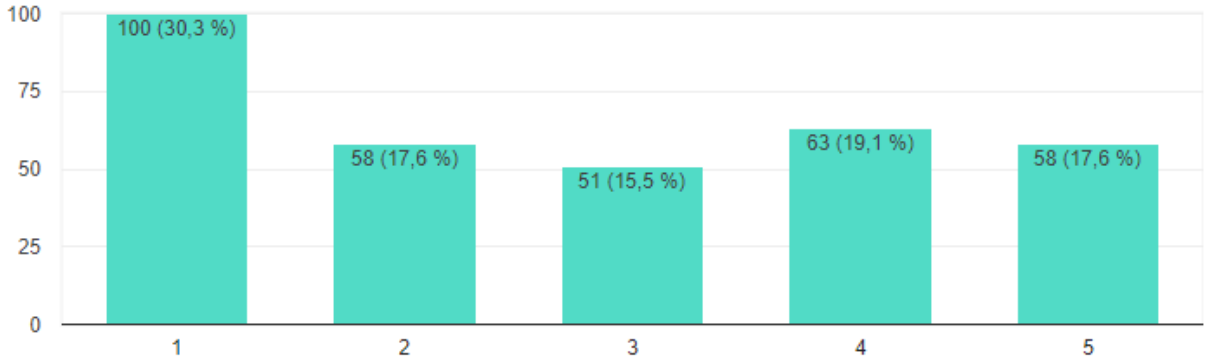
Grafikon 17.: Prikaz percepcije ispitanika o sigurnosti internetskih i bezgotovinskih transakcija prije COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Ispitanici s 44,2 i 32,4 posto većinski smatraju kako su internetske i bezgotovinske transakcije tijekom pandemije bile dovoljno sigurne, dok ih 20 posto ne može odrediti. Tek 3,3 posto ispitanika misli da internetske i bezgotovinske transakcije tijekom pandemije nisu bile dovoljno sigurne.

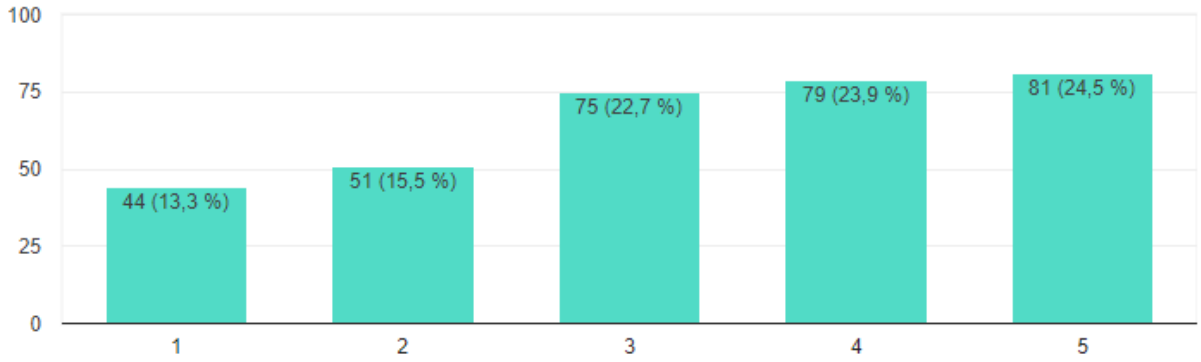
Grafikon 18.: Prikaz korištenja gotovine kao sredstva plaćanja za vrijeme COVID-19 pandemije zbog straha od zaraze



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Ispitanici većinski s 30,3 i 17,6 posto negiraju korištenje gotovine zbog straha od zaraze COVID_19 virusom, dok s druge strane njih 19,1 i 17,6 posto tvrdi da su iz tog razloga manje koristili gotovinu. Samo 15,5 posto ispitanika tvrdi kako nisu sigurni.

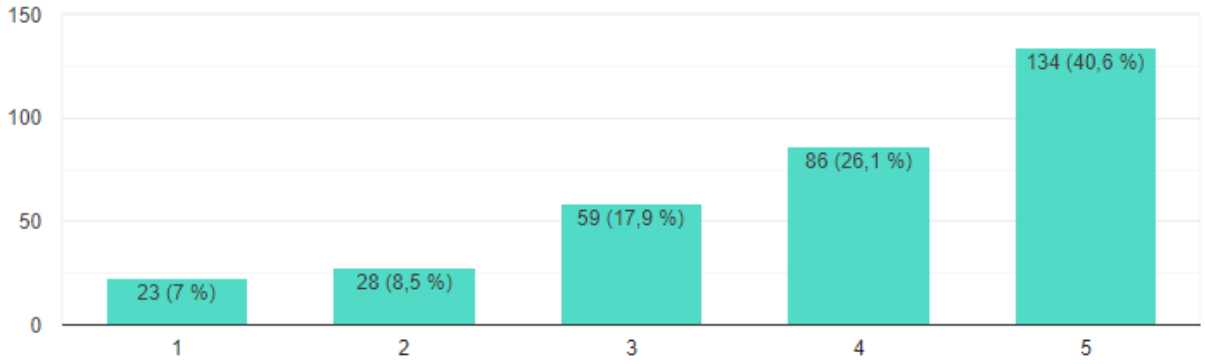
Grafikon 19.: Prikaz plaćanja primarno bezgotovinskim instrumentima zbog COVID-19 pandemije



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Većina ispitanika je s 24,5 i 23,9 posto odgovorila kako je upravo zbog pandemije primarno počela plaćati bezgotovinskim instrumentima. Na drugom mjestu su ispitanici koji nisu sigurni s 22,7 posto i oni koji zbog pandemije nisu počeli primarno plaćati bezgotovinskim instrumentima s 13,3 i 15,5 posto.

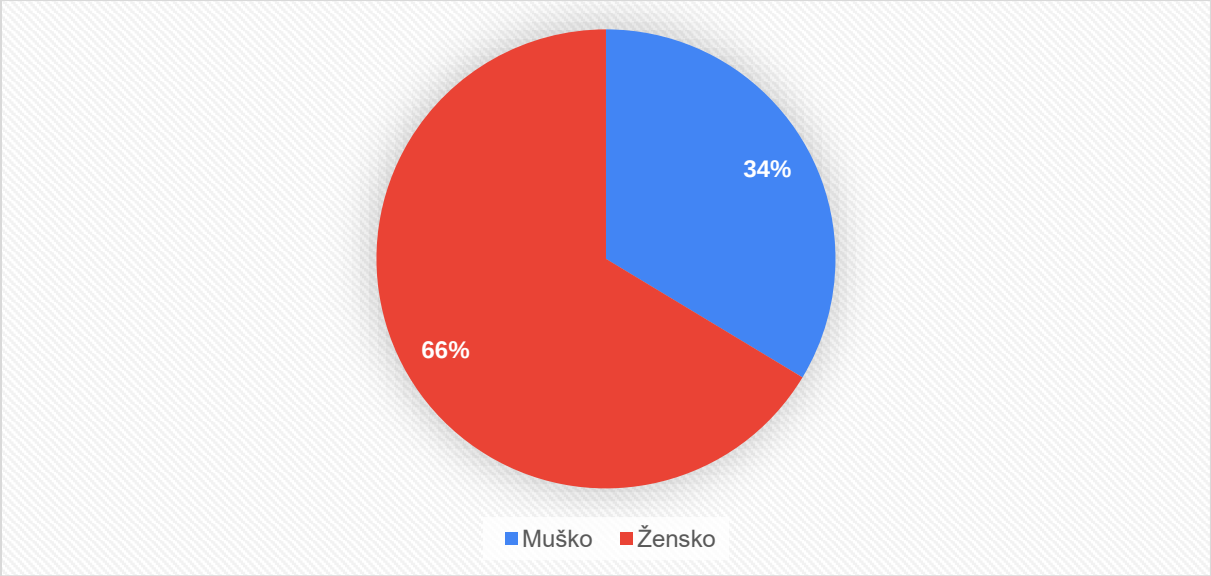
Grafikon 20.: Prikaz korisnika koji će i nakon COVID-19 pandemije primarno nastaviti plaćati s bezgotovinskim instrumentima.



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

S 40,6 i 26,1 posto većina ispitanika je odgovorila kako će i nakon pandmije nastaviti plaćati bezgotovinskim instrumentima, dok će tek manjina sa 7 i 8,5 posto nastaviti primarno plaćati gotovinom. Ostali ispitanici će nastaviti podjednako koristiti gotovinu i bezgotovinske instrumente plaćanja.

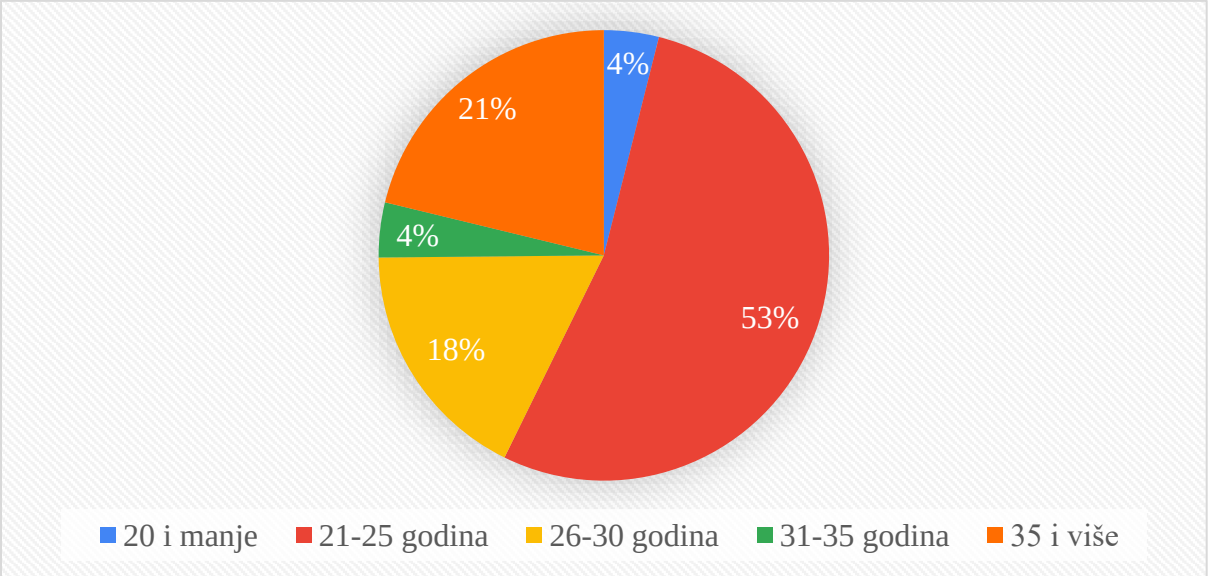
Grafikon 21.: Prikaz spolne strukture ispitanika



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Od uzorka veličine 330 ispitanika, 219 čine žene (66,4 posto), a 111 čine muškarci (33,6 posto).

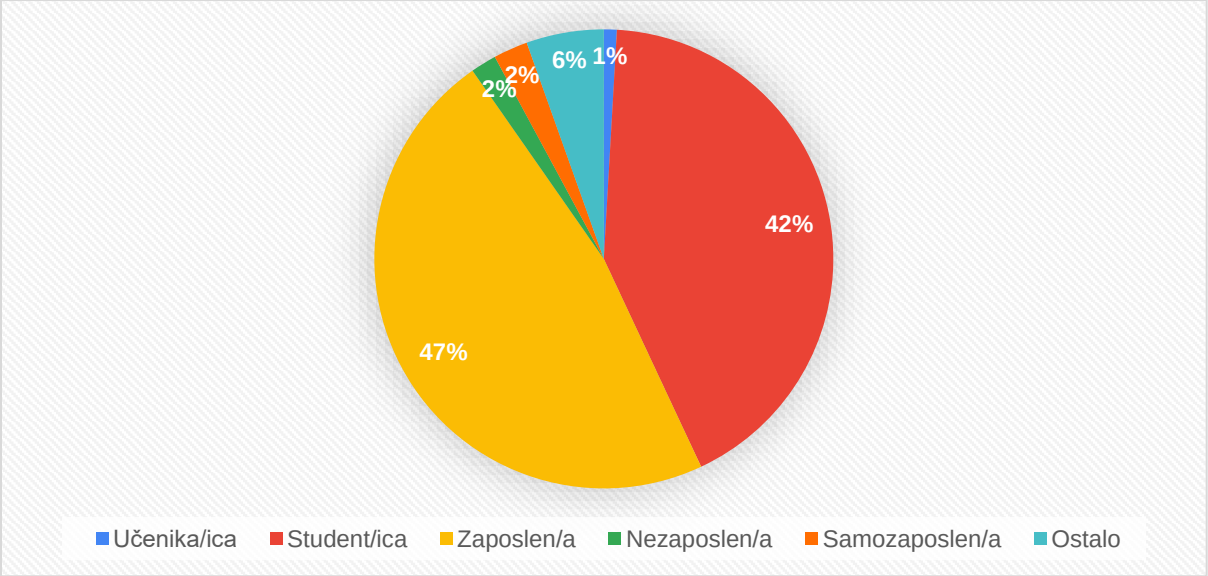
Grafikon 22.: Prikaz dobne strukture ispitanika



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Više od polovice ispitanika pripada dobnoj skupini između 21 i 25 godina, njih 53,3 posto, sljedeća najzastupljenija s 21,2 posto je dobna skupina iznad 35 godina. Nakon toga sljedeća najzastupljenija skupina s 17,6 posto je od 26-30 godina, dok su jednako zastupljene skupine ona od 31 do 35 godina te skupina od 20 i manje godina, svaka s 3,9 posto.

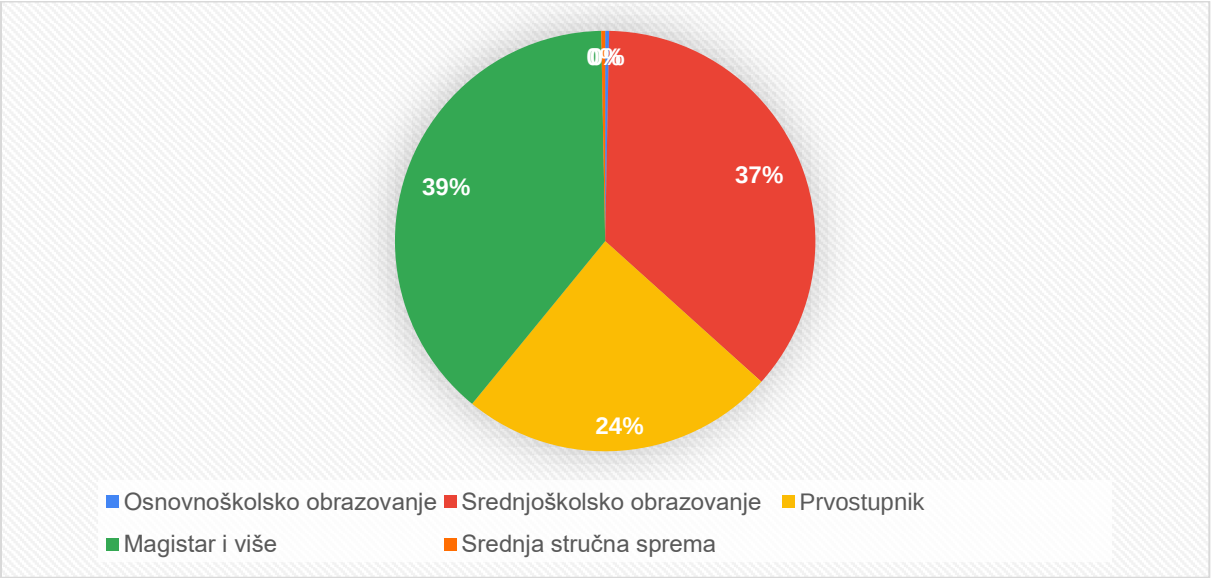
Grafikon 23.: Prikaz statusa zaposlenosti kod ispitanika



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

Najviše ispitanika s 47,3 posto je zaposleno, dok 42,1 posto ispitanika čine studenti. Nezaposleni čine 1,8 posto uzorka, dok se ostatak uzorka od 8,8 posto sastoji od učenika, samozaposlenih i umirovljenika.

Grafikon 24.: Prikaz stupnja obrazovanja kod ispitanika



Izvor: izrada autora na temelju podataka prikupljenih u istraživanju

U uzorku najviše ispitanika s 38,8 posto čine magistri, dok je sljedeća najzastupljenija skupina sa srednjoškolskim obrazovanjem s 36,4 posto. Prvostupnici su treći najzastupljeniji s 24,2 posto te ostatak uzorka čine ispitanici s osnovnoškolskim obrazovanje.

5.6 Rasprava o rezultatima istraživanja

Većina ispitanika je odgovorila kako su prije i u doba COVID-19 pandemije često koristili bezgotovinska sredstva te preferirali bezgotovinske transakcije i internetsku kupovinu. Dio ispitanika odgovorio je da su više kupovali preko interneta dok ih je dio sve transakcije provodio putem interneta, njih 4,5 posto. Ovakvi rezultati su očekivani, obzirom da je većina fizičkih trgovina bilo zatvorenu za vrijeme trajanja *lockdown-a*. Odgovor na pitanje jesu li prilikom plaćanja internetskog ili drugog bezgotovinskog plaćanja u doba pandemije bili ili pokušani biti prevareni, ispitanici su s 11,2 posto odgovorili da nisu sigurni - što je povećanje od 8,5 posto u odnosu prije pandemije. Takav odgovor je očekivan obzirom da se za vrijeme pandemije povećao obujam prometa i broj *cyber* napada te je moguće da je prilikom provođenja transakcija prekinuta, no ispitanici nisu mogli prepoznati zašto je prekinuta. Više od polovice ispitanika odgovorilo je kako je u vrijeme pandemije bilo češće traženo da potvrdi svoj identitet prilikom bezgotovinskih transakcija, njih 50,6 posto što ukazuje na povećanje mjera zaštite. Ispitanici smatraju kako su u vrijeme pandemije bezgotovinske transakcije bile dovoljno

sigurne. Percepcija ispitanika o povećanju internetskih prijevara za vrijeme pandemije dovoljno govori podatak da ih s 41,8 posto većina nije sigurna, dok je druga najzastupljenija skupina s 21,2 i 11,5 posto ipak primijetila povećanje istih.

Rezultate ovog istraživanja uspoređeni su s rezultatima sličnih istraživanja kako bi se što jasnije prikazao trend određenih dijelova rezultata. Istraživanje Odjela za digitalizaciju, kulturu, medije i sport Ujedinjenog Kraljevstva (2021.) anketiralo je mala, srednja i velika poduzeća kako bi saznali je li *cyber* kriminal stvarno u porast i jesu li primijetili napade na svoju organizaciju. Istraživanje potvrđuje kako *cyber* kriminal stvarno je u porastu u 2020. godini, jer su ga primijetila većina poduzeća, njih 46 posto. Uzorak istraživanja iznosi 1 419 poduzeća, velikih, malih i srednjih poduzeća što čini uzorak reprezentativnim. Istraživanje Utjecaja COVID-19 pandemije na financijske zločine i regulatornu usklađenost Fakulteta te instituta za računovodstvu iz Malezije (2021.) pokazalo je kako se u uzorku ukupnih financijskih kriminalnih radnji, fizički kriminal smanjio, dok se povećao *cyber* kriminal. „U Deloitte-ovom istraživanju o utjecaju COVID-19 pandemije u Europi na financijsku industriju zabilježeni su sljedeći rezultati. Tijekom rujna i studenog 2020. provedeni su razgovori s njihovim klijentima diljem Europe, Bliskog istoka i Afrike kako bi prikupili njihova mišljenja o utjecaj COVID-19 na platnu industriju i njihov strateški odgovor. Anketa je provedena pedeset poduzeća u sedam europskih zemalja: Ujedinjeno Kraljevstvo, Irska, Francuska, Njemačka, Italija, Španjolska i San Marino. Rezultati istraživanja su sljedeći: 44 posto ispitanih tvrtki bile su banke, građevinska društva (hipotekarne banke) ili druge kreditne institucije, 46 posto bili su dobavljači usluga, pružatelji tehničkih usluga, 10 posto su bile banke koje su stjecale druge banke, većina je bila univerzalna ili pretežito usmjerena na malo, a ograničen broj bio je usmjeren na korporativna plaćanja. U Italiji su intervjuirane tvrtke bile: dvije među vodećim bankovnim skupinama, industrijsko poduzeće talijanskog sektora financijskih usluga, partner jedne banke koji pruža ICT usluge, međunarodna tehnološka tvrtka. Ispitanici su izvučeni iz velikog broja viših uloga. Najčešće su to bili „šefovi“ poslovnih područja, uključujući one odgovorne za plaćanje: operacije, otpornost i kontinuitet poslovanja i proizvod. Anketa je strukturirana u četiri dijela: općenito, operacije i prijevara, promjena i transformacija, strateški utjecaj. Rezultati ankete su sljedeći: gotovo 60 posto ispitanika očekuje smanjenje potrošnje gotovine do 30 posto kada pandemija prestane kao ponašanje potrošača prema usvajanju beskontaktno, digitalnog i mobilnog plaćanje koje je sve učestalije. Na pitanje jesu li iskusili nastupanje operacijskih rizika 68 posto Europskih banaka odgovorilo je kako nije iskusilo nastupanje takvih rizika. Na pitanje jesu li mjere zaštite njihove organizacije dovoljne za brzu tranziciju na digitalna i *real-time* plaćanja, 58 posto ispitanika iz Europe odgovorilo je kako je

spremno no uz manje zapreke“ (Deloitte, 2020.).[68] Usporedba rezultata ostalih istraživanja s rezultatima dobivenim u Istraživanju o percepciji korisnika o zaštiti bezgotovinskih transakcija istraživanja potvrđuju trendove kretanja bezgotovinskih plaćanja i *cyber* rizika u doba pandemije.

Ovakvi rezultati dobiveni ovim istraživanjem ukazuju da su ispitanici i korisnici bezgotovinskih instrumenata te internetskih trgovine ipak primijetili određene promijene poput povećanje prijevara prilikom provođenja transakcija. Većina ljudi također je primarno plaćala bezgotovinskim instrumentima te će nastaviti i nakon pandemije, što je potkrijepljeno Deloitte-ovim istraživanjem. Također, važno je naglasiti da ih je i više od polovice primijetilo, kako su mjere zaštite prilikom provođenja transakcija bile strože i učestalije, nego prije COVID-19 pandemije.

5.7 Ograničenja i preporuka za buduća istraživanja

Istraživanje provedeno za pisanje ovog diplomskog rada precizno je prikazalo način na koji različiti korisnici percipiraju sigurnost bezgotovinskih transakcija prije i u doba COVID-19 pandemije, što je i bio temeljni cilj istraživanja, no anketni upitnik kao metoda istraživanja ipak ima ograničenja od kojih se u ovom upitniku posebno izdvaja jedno.

Naglasak je na razumijevanju novih tehnologija ili pojmova u pitanjima kod starijih dobnih skupina, što može utjecati na ispravnost njihovih odgovora te u konačnici na rezultate istraživanja. Anketa bi trebala sadržavati pitanja i pojmove koji bi svim dobnih skupinama trebala biti razumljiva ili ukoliko se autoru čini da je određeni pojam dovoljno nepoznat starijim dobnim skupinama, utoliko bi se isti pojam trebao pokušati kratko objasniti unutar pitanja navodeći primjer tog pojma.

[68] Deloitte (2020.), European COVID-19 Survey – Result Highlights, preuzeto 10. rujna 2021. s https://www2.deloitte.com/content/dam/Deloitte/it/Documents/financial-services/Deloitte_COVID%20Survey%20on%20Payment%20Services_IV2020.pdf

6. Zaključak

Uslijed porasta korištenja internetskih tehnologija i informacijskih sustava u zadnjih petnaest godina u svakodnevnom poslovanju i svim sektorima djelatnosti, a posebno u bankarskom sektoru sve veća pažnja pridodaje se sigurnosti i zaštiti istih. Nastankom najveće suvremene svjetske krize od Drugog svjetskog rata uzrokovane pojavom koronavirusa uslijedio je i povećan opseg „prisilne" digitalizacije poslovanja i razdoblje navikavanja na „novo normalno". Iako na prvi pogled posljedica ubrzane i „prisilne" digitalizacije poslovanja mnogim kako, ljudima tako i organizacijama predstavlja nešto pozitivno poput nove mogućnosti rada od kuće ili uštede zbog smanjenja troškova fizičkog poslovanja, s druge strane javljaju se novi rizici poslovanja kojima se do pojave pandemije nije pridavala velika pažnja te je njihova značajnost bila puno manja. Povećanje sigurnosnih i *cyber* rizika uvelike je utjecalo na suvremeno poslovanje i prije pandemije, dok je uslijed nastupanja iste došlo do velikog povećanja značajnosti određenih rizika nego u vrijeme prije.

Cilj rada bio je analizirati sigurnosne rizike i provesti istraživanje o zaštiti bezgotovinskih transakcija među korisnicima, kako bi se objasnila uspješnost provedbe donesenih sigurnosnih mjera u doba COVID-19 pandemije i time odrediti mjeru uspješnosti sigurnosti platnog prometa u doba COVID-19 pandemije.

Analiza sigurnosnih rizika pokazala je, kako su određeni rizici imali veću ili manju značajnost u doba pandemije, nego prije nje. Tako su najznačajniji rizici u doba pandemije bili rizici provedbe poslovnih procesa ili transakcijski informatički rizici te infrastrukturni informatički rizici. Česti *cyber* napadi na financijske institucije rezultirali su prekidom ili nekim oblikom obustave poslovanja i time predstavljaju ozbiljnu prijetnju poslovanju i naglašavaju važnost prevencije takvih događaja. Informacijski sustavi u današnjim financijskim institucijama i cjelokupnom platnom prometu glavni su nositelji poslovanja i kada su narušeni, izravno i u velikoj mjeri utječu na prihode i reputaciju organizacije.

Veća značajnost rizika u doba pandemije svakako se odnosi na sigurnost bezgotovinskih transakcija i njihovu provedbu, obzirom da je takav oblik plaćanja bio primaran u doba *lockdowna* i općenito za vrijeme pandemije. Istraživanje o percepciji korisnika o zaštiti bezgotovinskih plaćanja u doba pandemije potvrdilo je, kako većina misli da su transakcije za vrijeme pandemije bile dovoljno sigurne usprkos povećanom obujmu prometa i broju pokušaja

prijevara. Time se može zaključiti kako je bitna stavka cjelokupnog platnog prometa koja se odnosi na sigurnost fizičkih osoba dovoljno sigurna.

Mjere sigurnosti donesene od raznih institucija, kako regulatornih tako i institucija važnih za sigurnu provedbu transakcija, također, su se pokazale učinkovite obzirom na nepovoljnu gospodarsku situaciju. Najbolji primjer za to je povećanje kontrola prilikom provođenja transakcija i učestalije provjere identiteta kojeg su primijetili i ispitanici u istraživanju. Mjere regulatornih institucija, također, su pokazale svoju učinkovitost i na razini očuvanja likvidnosti financijskog sustava te neometanosti poslovanja.

Odgovorno upravljanje zaštitom i sigurnosti informacijskih sustava važan je čimbenik uspješnog poslovanja svake ozbiljne organizacija, naročito onih u financijskom sektoru. Važnost tog čimbenika očituje se u vremenu pandemije i događanjima koja su nastupila u zadnjem desetljeću, u kojem je dokazano kako su poduzeća koja uspješno upravljaju zaštitom i sigurnošću informacijskih sustava otpornija od onih koji „čekaju“ da se dogodi negativan događaj pa tek onda nastoje popraviti, često nenadoknadivu materijalnu i važniju reputacijsku štetu koja izravno utječe na dugoročno poslovanje i samu vrijednost poduzeća. Cjelokupni platni promet u ovoj krizi pokazao je dobru otpornost unatoč novim rizicima, na koje i u budućnosti valja obratiti pažnju.

Kada se sve sažme važno je napomenut, kako zaštitom i sigurnošću informacijskih sustava treba aktivno upravljati, prije svega na način da se poduzimaju prevencijske zaštitne mjere i prate kako trendovi u razvoju tehnologije, tako i trendovi kretanja sigurnosnih rizika koji se brzo izmjenjuju.

Popis literature

1. Bača, M. (2004.), Uvod u računalnu sigurnost, Narodne novine, Zagreb
2. BBC (2021.), China accused of cyber-attack on Microsoft Exchange servers, preuzeto 7. rujna s https://www.bbc.com/news/world-asia-china-57889981
3. Berman, S., J., Kesterson-Townes, L., Marshall, A., Sirvathsa, R. (2012.), How cloud computing enables process and business model innovation, preuzeto 2. rujna 2021. s https://www.emerald.com/insight/content/doi/10.1108/10878571211242920/full/html
4. Bezhovski, Z. (2016.), The Future of the Mobile Payment as Electronic Payment System, European Journal od Business and Management, 8(8), 128.-129. str., https://core.ac.uk/download/pdf/234627158.pdf
5. BIS (2021.), E-commerce in the pandemic and beyond, preuzezo 7. rujna 2021. s https://www.bis.org/publ/bisbull36.pdf
6. Bloomberg (2021.), CNA Financial Paid $40 Million in Ransom After March Cyberattack, preuzeto 7. rujna s https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack
7. Briedis H., Ungerman K., Kronschnabl A., Rodriguez A. (2020.), Adapting to the next normal on retail: The Customer experience imperative, prezueto 2. rujna 2021. s https://www.mckinsey.com/industries/retail/our-insights/adapting-to-the-next-normal-in-retail-the-customer-experience-imperative
8. Bruno, P., Dencker, O., Niederkorn, M. (2020.), Accelerating winds of change in global payment, preuzeto 3. rujna 2021. s https://www.mckinsey.com/industries/financial-services/our-insights/accelerating-winds-of-change-in-global-payments
9. Carnegie endowment for international peace (2021.), Timeline of Cyber Incidents Involving Financial Institution, preuzeto 10. rujna 2021. s https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
10. CARNeT, LS&S (2005.), Phising napadi, preuzeto 6. rujna s https://www.cis.hr/www.edicija/Phishingnapadi.html
11. CISA (2021.), Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses, preuzeto 10. rujna 2021. s https://www.cisa.gov/sites/default/files/publications/CISA%20Insights_Guidance-for-MSPs-and-Small-and-Mid-sized-Businesses_S508C.pdf

12. CISOMAG (2021.), Credit card data of 10,000 American Express accounts posted on Darknet Forum for free, preuzeto 10. rujna 2021. s https://cisomag.eccouncil.org/american-express-credit-card-data-sale-on-darknet/
13. Clarida, H., R., Duygan-Bump, B., Scotti, C. (2021.), The COVID-19 Crisis and the Federal Reserve's Policy Response., preuzeto 11. rujna 2021. s https://www.federalreserve.gov/econres/feds/files/2021035pap.pdf
14. Culp, L., C. (2001.), The Risk Management Process – Business Strategy, and Tactics, John Wiley & Sons
15. Deloitte (2020.), European COVID-19 Survey – Result Highlights, preuzeto 10. rujna 2021. s https://www2.deloitte.com/content/dam/Deloitte/it/Documents/financial-services/Deloitte_COVID%20Survey%20on%20Payment%20Services_IV2020.pdf
16. Department for digital, culture, media & sport (2021.), Cyber security breaches survey 2021., preuzeto 6. rujna s https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf
17. EBA (2020.), EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic, preuzeto 10. rujna 2021. s https://www.eba.europa.eu/eba-provides-additional-clarity-on-measures-mitigate-impact-covid-19-eu-banking-sector
18. ECB (2010.) The payment system – payments, securities and derivatives, and the role of eurosystem, preuzeto 30. kolovoza 2021. s https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf
19. ECB (b.d.) Electronic money, preuzeto 31. kolovoza 2021. s https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html
20. Egerth, K. (2021.), Cash is no longer king in times of COVID-19, preuzeto 7. rujna s https://www2.deloitte.com/ch/en/pages/consumer-industrial-products/articles/cash-is-no-longer-king-in-times-of-covid19.html
21. EMVCo (2016.), EMV 3-D Secure, preuzeto 10. rujna 2021., s https://www.emvco.com/emv-technologies/3d-secure/
22. ESRB (2020.) Systemic cyber risk, preuzeto 14. rujna 2021. s https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
23. Hamdi, H. (2007.), Problemi razvoja elektroničkog novca, Financijska teorija i praksa 31(3), 291. str. https://hrcak.srce.hr/18214

24. HNB (2015.) EuroNKS, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/euronks

25. HNB (2015.) Hrvatski sustav velikih plaćanja, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/hsvp
26. HNB (2015.) Nacionalni klirinški sustav, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/nks

27. HNB (2015.) O platnom prometu, preuzeto 30. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/o-platnom-prometu
28. HNB (2015.) TARGET2, preuzeto 31. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/platni-sustavi/target2

29. HNB (2020.) O platnom prmetu, preuzeto 30. kolovoza 2021. s https://www.hnb.hr/temeljne-funkcije/platni-promet/o-platnom-prometu
30. HNB (2020.), HNB preporučuje povećanje maksimalnog iznosa beskontaktne platne transakcije bez primjene PIN-a sa 100 na 250 kuna, preuzeto 7. rujna 2021. s https://www.hnb.hr/-/hnb-preporucuje-povecanje-maksimalnog-iznosa-beskontaktne-platne-transakcije-bez-primjene-pin-a-sa-100-na-250-kuna
31. HNB (2020.), HNB preporučuje povećanje maksimalnog iznosa beskontaktne platne transakcije bez primjene PIN-a sa 100 na 250 kuna, preuzeto 7. rujna 2021. s https://www.hnb.hr/-/hnb-preporucuje-povecanje-maksimalnog-iznosa-beskontaktne-platne-transakcije-bez-primjene-pin-a-sa-100-na-250-kuna
32. HNB (2020.), HNB preporučuje privremeno ukidanje naknada za podizanje gotovine na bankomatima izvan vlastite bankomatske mreže, preuzeto 7. rujna 2021. s https://www.hnb.hr/-/hnb-preporucuje-privremeno-ukidanje-naknada-za-podizanje-gotovine-na-bankomatima-izvan-vlastite-bankomatske-mreze
33. HNB (2020.), Mjere Hrvatske narodne banke za ublažavanje ekonomskih posljedica pandemije, preuzeto 10. rujna 2021. s https://www.hnb.hr/documents/20182/2953147/hn170320_prezentacija_Vujcic.pdf/bc719a93-ba7b-26ba-626e-950cf32dcf7f?t=1584467194434
34. HNB (2020.), *Mjere Hrvatske narodne banke za ublažavanje ekonomskih posljedica pandemije* [e-publikacija], preuzeto s https://www.hnb.hr/documents/20182/2953147/hn170320_prezentacija_Vujcic.pdf/bc719a93-ba7b-26ba-626e-950cf32dcf7f?t=1584467194434

35. HNB (2020.), Ukupna vrijednost bezgotovinskih transakcija u pet se godina povećala za 47 posto, preuzeto 1. rujna 2021. s: https://www.hnb.hr/-/ukupna-vrijednost-bezgotovinskih-transakcija-u-pet-se-godina-povecala-za-47-posto
36. HNB (2021.), Platne kartice i kratične transakcije, [e-publikacija], preuzeto 3. rujna 2021. s https://www.hnb.hr/analize-i-publikacije/redovne-publikacije/platne-kartice-i-karticne-transakcije
37. ISACA (2015), Global Cyber Security Status Report, ISACA, Roling Meadows, Illinois, USA
38. Lund, S., Mehta, A., Manyka, J., Goldshtein, A. (2018.), A decade after the global financial crysis: What has (and hasn't) changed?, preuzeto 2. rujna 2021. s https://www.mckinsey.com/industries/financial-services/our-insights/a-decade-after-the-global-financial-crisis-what-has-and-hasnt-changed
39. Lund, S., Madgavkar, A., Manyika, J., Smit,S., Ellingrud, K., Robinson O. (2021.), The future of work, after the COVID-19, preuzeto 10. rujna 2021., s https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19
40. Miloš Sprčić, D. (2013.) Upravljanje rizicima – temeljni koncepti, strategija i instrumenti, Zagreb, Sinergija
41. Mišić., T. (2021.), Utjecaj pandemije COVID-19 na navike plaćanja u RH, preuzeto 1. rujna 2021. s https://www.hnb.hr/-/utjecaj-pandemije-covid-19-na-navike-placanja-u-rh
42. Mišić., T. (2021.), Utjecaj pandemije COVID-19 na navike plaćanja u RH, preuzeto 3. rujna 2021. s https://www.hnb.hr/-/utjecaj-pandemije-covid-19-na-navike-placanja-u-rh
43. Newman, H., L. (2020.), Online Credit Card Skimmers Are Thriving During the Pandemic,preuzeto 7. rujna 2021. s https://www.wired.com/story/magecart-credit-card-skimmers-coronavirus-pandemic/
44. OECD (2020.), E-commerce in the time of COVID-19, preuzeto 2. rujna 2021. s https://read.oecd-ilibrary.org/view/?ref=137_137212-t0fjgnerdb&title=E-commerce-in-the-time-of-COVID-19&_ga=2.62472940.1345077669.1630588043-2051317201.1630494535
45. Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010. on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board.
46. Spremić, M. (2017.), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb: Ekonomski fakultet

47. Swiss National Bank (2020.) Payments and cash withdrawals, preuzeto 3. rujna 2021. s https://data.snb.ch/en/topics/finma#!/cube/zavezaka?fromDate=2020-01&toDate=2021-01&dimSel=D0(T0,DZ0,T1,DZ1)
48. Teh, P.S., Zhang, N. Teoh, A.B.J. and Chen, K. (2016), "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices", *International Journal of Pervasive Computing and Communications*, Vol. 12 No. 1, pp. 127-153. https://doi.org/10.1108/IJPCC-01-2016-0005
49. The Seattle Times (2021.), Hack of Seattle payments processing firm puts local governments on alert, preuzeto 7. rujna s https://www.seattletimes.com/seattle-news/hack-of-seattle-payments-processing-firm-puts-local-governments-on-alert/
50. Undale, S., Kulkarni, A. and Patil, H. (2021.), Perceived eWallet security: impact of COVID-19 pandemic, *Vilakshan - XIMB Journal of Management*, Vol. 18 No. 1, pp. 89-104. https://doi.org/10.1108/XJM-07-2020-0022
51. United Nations Development Programme (2020.), COVID-19 pandemic, preuzeto 1. rujna 2021. s https://www.pacific.undp.org/content/pacific/en/home/coronavirus.html
52. Wenjie, C., Mrkaic. M., Nabar, S., M. (2019.), The Global Economic Recovery 10 Years After the 2008 Financial Crisis, preuzeto 1. rujna 2021. s https://www.imf.org/en/Publications/WP/Issues/2019/04/26/The-Global-Economic-Recovery-10-Years-After-the-2008-Financial-Crisis-46711
53. World Health Organization (2020.), WHO Director-General's opening remarks at the media briefing on COVID-19 - 13 August 2020, preuzeto 2. rujna 2021. s https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---13-august-2020
54. World Health Organization (2021.), Global Study of Origins of SARS-CoV-2: China Part, preuzeto 1. rujna 2021. s https://www.who.int/publications/i/item/who-convened-global-study-of-origins-of-sars-cov-2-china-part
55. Zakon o elektroničkom novcu, Narodne novine br. 66/2018., (2018.)
56. Zakon o platnom prometu, Narodne novine br. 66/2018. (2018.)
57. Zavod za sigurnost informacijskih sustava, (2020.), Phising poruke elektroničke pošte [e-publikacija], preuzeto 6. rujna s: https://www.zsis.hr/default.aspx?id=428
58. ZSIS (2020.), Upozorenje o phising kampanji na temu COVID-19, preuzeto 10. rujna 2021. s https://www.zsis.hr/default.aspx?ID=435

Popis slika

Popis tablica

Popis grafikona

Prilozi

Prilog 1. Pitanja anketnog upitnika

Pitanja koja se odnose na stanje prije pandemije:

1. Koliko često obavljate bezgotovinske transakcije?
   a) svaki dan
   b) 2-3 puta tjedno
   c) jedanput mjesečno
   d) ostalo

2. Preferirate li bezgotovinske transakcije i internetsku kupovinu?
   a) da
   b) ne
   c) nisam sigurna/siguran

3. Prije COVID-19 pandemije bio sam žrtva prijevare/krađe prilikom bezgotovinskog plaćanja.
   a) da
   b) ne
   c) nisam sugurna/siguran

Ocjenite sljedeće tvrdnje ocjenom od 1 do 5:

1 - uopće se ne slažem

2 - ne slažem se

3 - niti se slažem, niti se ne slažem

4 - slažem se

5 - u potpunosti se slažem

4. Preferiram bezgotovinska plaćanja i internetsku kupovinu zbog sigurnosti podataka.
5. Prije COVID-19 pandemije sam često koristio/la bezgotovinska sredstva plaćanja.
6. Smatram da je bezgotovinsko plaćanje pouzdan način plaćanja.
7. Mislim da je prije pandemije bilo manje internetskih prijevara.
8. I nakon pandemije ću primarno kupovati bezgotovinskim sredstvima te putem Interneta, jer sam zadovoljan/la razinom sigurnosti.

Pitanja koja se odnose na transakcije u vrijeme COVID-19 pandemije:

9. Koji Vam je preferirani bezgotovinski način plaćanja za vrijeme COVID-19 pandemije?
   a) digitalni novčanik npr. Google pay, Apple pay
   b) kartice
   c) kriptovalute
   d) ostalo mobilno internet bankarstvo

10. Jeste li za vrijeme pandemije više kupovali preko interneta, ako da koliko često?
    a) da
    b) ne
    c) sve transakcije sam obavljao preko interneta
    d) ostalo

11. Jeste li bili ili pokušani biti prevareni prilikom internetskog ili drugog bezgotovinskog plaćanja tijekom COVID-19 pandemije?
    a) da
    b) ne
    c) Nisam siguran
    d) ostalo

12. Jeste li tijekom COVID-19 pandemije bili češće traženi da se autenticirate (potvrdite svoj identitet putem pina/tokena/jednokratne zaporke) prilikom internetskog ili bezgotovinskog plaćanja?
    a) da
    b) ne
    c) nisam siguran
    d) ostalo

13. Koliki je iznos najveće bezgotovniske transakcije koju ste napravili u doba COVID-19 pandemije?
    a) 500-1000 kn
    b) 1000-2000 kn
    c) 2000-4000 kn
    d) više od 5000 kn

14. Je li Vam banka odbila bezgotovinsku transakciju prilikom plaćanja u doba pandemije zbog sumnje na prijevaru?
    a) da
    b) ne
    c) nisam siguran

15. Koliko često Vam se u vrijeme COVID-19 pandemije dogodila greška u plaćanju zbog koje niste mogli do kraja izvršiti transakciju?
    a) jedanput
    b) 1-2 puta
    c) više od 3 puta
    d) tijekom pandemije mi se nikada nije dogodila greška u transakciji

16. Jeste li upoznati sa smjernicama ili odlukama o sprječavanju prijevara prilikom bezgotovinskih i internetskih plaćanja u doba COVID-19 pandemije?
    a) da
    b) ne
    c) čuo sam nešto o tome, ali nisam siguran

Ocijenite sljedeće tvrdnje ocjenom od 1 do 5:

1 - uopće se ne slažem

2 - ne slažem se

3 - niti se slažem, niti se ne slažem

4 - slažem se

5 - u potpunosti se slažem

17. Smatram da su internetske i bezgotovinske transakcije tijekom COVID-19 pandemije bile dovoljno sigurne.
18. U doba pandemije manje sam koristila/koristio gotovinu zbog opreza da se ne zarazim COVID-19 virusom?
19. U doba COVID-19 pandemije počeo sam primarno plaćati bezgotovinskim instrumentima.
20. Nakon COVID-19 pandemije nastavit ću primarno plaćati bezgotovinskim instrumentima.

Demografski podaci:

21. Spol
    a) Muško
    b) Žensko

22. Dob
    a) 20 i manje
    b)21 – 25 godina
    c) 26 – 30 godina
    d) 31 – 35 godina
    e) 35 i više

23. Koji je vaš trenutni status vezan uz zaposlenost
    a) učenik
    b) student
    c) zaposlen
    d) nezaposlen
    e) samozaposlen

24. Vaše obrazovanje
    a) Osnovnoškolsko obrazovanje
    b) Srednjoškolsko obrazovanje
    c) Prvostupnik
    d) Magistar i više