Водич за **дигитална плаћања**

MAJ 2022

Centralna banka BOSNE I HERCEGOVINE
Централна банка БОСНЕ И ХЕРЦЕГОВИНЕ
WORLD BANK GROUP
Finance, Competitiveness & Innovation

САДРЖАЈ

Фото кредит: https://www.pexels.com/@pavel-danilyuk/

1. УВОД

Развојем и технолошким напретком друштва јављају се нове потребе финансијских корисника и стварају нови изазови на финансијском тржишту. Један од новијих догађаја је појава нових опција плаћања за обављање финансијских трансакција. Поред класичног готовинског плаћања, уз подршку савремених технологија развијају се и различити облици дигиталног, безготовинског плаћања. Пандемија КОВИД-19 учинила је дигитално плаћање још практичнијим у односу на традиционалне начине плаћања, првенствено због могућности смањења преноса вируса. С обзиром на даљи развој технологије, очекује се да ће ови начини плаћања и трансфера новца повећати свој удио у укупним плаћањима.

У овом водичу ћемо се фокусирати на најновије трендове у дигиталном, безготовинском плаћању доступном грађанима у Босни и Херцеговини. На тржишту су све чешће различите врсте безготовинског плаћања, а динамика и брзина развоја намећу потребу за повећањем едукације и свијести јавности како би се безготовинско плаћање могло одговорније и сигурније користити.

Дигитална плаћања су безготовинске трансакције, односно плаћања роба и услуга која се одвијају искључиво у датом електронском/виртуелном окружењу.

Главна карактеристика безготовинског плаћања је да се трансакција одвија без физичког трансфера новца. То значи да и платилац (особа која плаћа) и прималац плаћања (прималац који прима новац) немају контакт са готовином. Предност дигиталног плаћања огледа се у томе што платилац може извршити плаћање у било које вријеме, без обзира на локацију, на брз и једноставан начин, користећи одабрана технолошка рјешења (нпр. посебну мобилну апликацију или цијели пакет услуга – мобилно и/или интернет банкарство)..

Дигитализација услуга захтијева едукацију корисника финансијских плаћања како би могли на сигуран и одговоран начин користити савремене платне услуге. Једнако је важно едуковати потрошаче о њиховим правима и могућностима за отклањање потенцијалне злоупотребе и случајева преваре у вези с дигиталним плаћањем. У том смислу, у наставку ће се детаљније говорити о најновијим тржишним трендовима везаним за мобилно и бесконтактно плаћање и његовим карактеристикама, укључујући различите приступе дигиталном плаћању у БиХ, основне врсте дигиталног плаћања, техничке захтјеве и обавезе корисника, као и информације о лажним или обмањујућим праксама којих би корисници плаћања требали бити свјесни. Такође, водич ће понудити информације о правима потрошача, објаснити процедуре за подношење рекламација, те навести надлежне бх. институције за заштиту права потрошача.

Фото кредит: https://www.freepik.com/rawpixel-com

2. ТЕМАТСКИ ДИО – Врсте дигиталних плаћања и заштита права потрошача

2.1. Различити приступи дигиталном плаћању у БиХ

У Босни и Херцеговини су доступни различити модели, иновативни приступи и услуге за дигитално плаћање. Све банке у БиХ издају платне картице за плаћања (контактна и бесконтактна) преко Pont-of-Service (POS) терминала и путем интернета (у физичком и онлајн окружењу). Међутим, на тржишту су све присутније друге могућности. Основна подјела се може направити између апликација (apps) које су развиле комерцијалне финансијске институције попут банака и оних које служе као средство за плаћање услуга других компанија за куповину или пружене услуге. Свеукупно, циљ је омогућити једноставније, сигурније и брже плаћање, а значај се придаје и еколошким предностима кроз смањење употребе папира или других материјалних ресурса. Апликације посебну пажњу посвећују плаћању и сигурности похране података, па је важно бити свјестан рјешења која апликације нуде и да ли она одговарају нечијим потребама плаћања.

На примјер, неке компаније нуде посебну апликацију за плаћање својих услуга која је повезана са рачуном код банке партнера; корисник преузима апликацију са популарних сервиса, региструје се (са подацима о картици, одређеним личним подацима и референтним бројем услуге) и отвара рачун у банци како би апликација остала активна. Процес плаћања се углавном одвија кроз периодично креиране налоге (обавјештења о доспијећу плаћања) и нема потребе за одласком у банку или поновним уносом података за плаћање. Уобичајена је пракса да одређена апликација дозвољава плаћања вишеструким пружаоцима услуга. Финансијске институције пружају својим клијентима и различите опције дигиталног плаћања, стално ажурирају своју праксу, помажу у евидентирању трансакција и олакшавају њихову употребу (на примјер, додатни механизми заштите који покривају процес плаћања без потребе за потврђивањем потенцијално ризичних трансакција или метода складиштења података посебним позивима - токенизирани приступ или опција за управљање личним финансијама помоћу алата за обрачун трошкова итд.).

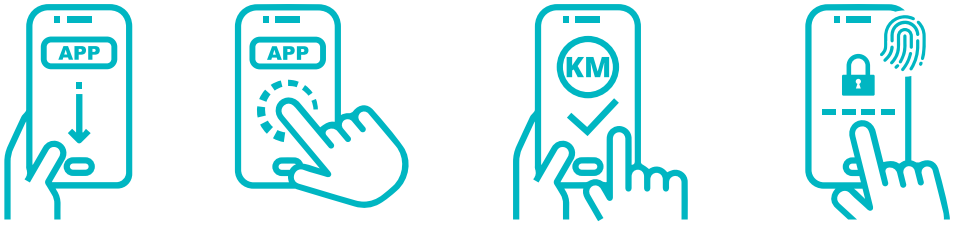
Опције дигиталног плаћања провјерите код свог финансијског или другог пружаоца услуга. Лакоћа или сложеност кориштења, брзина, додатне могућности плаћања, нижи трошкови за ову врсту плаћања, да ли је апликација доступна под условом отварања рачуна у посебној банци или је везана за другу врсту услуге итд. важна су питања о којима треба размишљати и тражити одговоре прије него што донесете одлуку о кориштењу дигиталног плаћања.

2.2. Шта су апликације за мобилно плаћање?

Апликације за мобилно плаћање (apps) су посебни софтверски програми креирани за паметне телефоне или таблете, који корисницима омогућавају различите врсте плаћања. Осим функционалности плаћања, ове апликације често омогућавају и друге функционалности као што су: провјера стања на рачуну, преглед трошкова, подношење онлајн апликација, маркетинг и учешће у промотивним кампањама, комуникација с пружаоцима финансијских услуга између осталих функционалности корисника.

На тржишту постоје различите врсте, а разликују се по начину на који пружају услуге платног промета. Посоји неколико опција плаћања, а најчешће су:

i) **Плаћање путем електронског налога за плаћање** врши се инсталисањем и покретањем апликације и почетним уносом додијељеног PIN-а или биометријских података (обично отиска прста). Апликације за плаћање већ садрже софтверски дефинисане елементе налога за плаћање које је потребно попунити зависно од врсте плаћања. Тиме се олакшава коришћење услуге. Најважнији елементи налога (који је изабрао и/или попунио корисник) су избор рачуна са којег се врши плаћање (само ако имате више налога), сврха плаћања, подаци о примаоцу уплате (назив/име и адреса), рачун примаоца уплате и износ уплате. Додатни елементи биће потребни само у случају међународних плаћања или плаћања јавних прихода. Креирани налог се потврђује поновним уносом PIN-а или биометрије, након чега се плаћање сматра обављеним.



Инсталација апликације › Покретање апликације PIN-ом или биометријским подацима › Попуњавање налога за плаћање › Одобрити плаћање PIN-ом или биометријским подацима

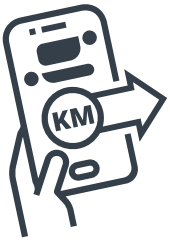
ii) **Апликације са могућношћу очитавања Quick Response (QR) кодова** који се налазе на фактурама продавца који дозвољавају ову врсту плаћања. Након покретања апликације потребно је одабрати опцију плаћања, скенирати QR код рачуна мобилним уређајем, те одобрити плаћање PIN-ом или биометријским подацима, након чега се плаћање сматра обављеним.

Покретање апликације › Одабрати опцију плаћања QR кодом › Скенирати QR код рачуна › Одобрити плаћање PIN-ом или биометријским подацима

iii) **Плаћање путем технологије комуникације блиског поља (NFC).** Ова опција значи да активирате ову функционалност унутар постојеће апликације за мобилно плаћање (као што је апликација за мобилно банкарство) или уносом других потребних података попут оних који се односе на вашу платну картицу, уз обавезну активацију NFC опције у поставкама мобилног уређаја. Плаћање вршите откључавањем мобилног телефона и стављањем задње стране мобилног уређаја на бесконтактни POS терминал, без обзира на то имате ли интернет конекцију или не. Важно је напоменути да апликацију није потребно покретати, али да бисте извршили плаћање обично је потребно унијети PIN картице на POS терминалу. На тај начин је омогућено плаћање без платне картице при руци.

Откључавање мобилног телефона

Стављање мобилног уређаја на бесконтактни POS терминал



iv) **Chat апликације** се могу прилагодити и за функционалност плаћања. Тренутно се најчешће користе за провјеру стања на рачуну, слање новца особама у вашем именику које су се регистровале за примање новца путем те апликације и плаћање унапријед дефинисаних рачуна (на примјер, комуналије, струја, гас, итд.). Износи трансакција су ограничени (на примјер на 200 KM), активација је често повезана с другом постојећом дигиталном услугом (као што је мобилно банкарство) и свако плаћање се провјерава уносом одговарајућег PIN-а.

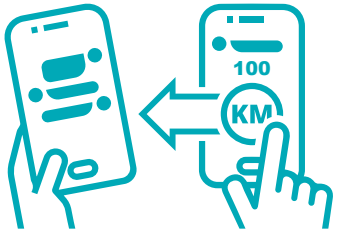


Foto kredit: https://unsplash.com/@jonasleupe

2.3. Активација и технички услови за коришћење апликација за мобилно плаћање

Плаћање се обично врши повезивањем апликације са вашим банковним рачуном или платном картицом. Активација апликације која је повезана с вашим банковним рачуном обично захтијева постојање уговорног односа између банке и власника рачуна уз прихватање услова коришћења, било као појединачне услуге било услуге у оквиру одређеног пакета услуга. Такве апликације укључују апликације за мобилно банкарство, апликације за chat банкарство и друге специјализоване банкарске апликације.

Активација апликације која је повезана с платном картицом обично подразумијева онлајн регистрацију корисника, уз прихватање услова коришћења и почетни унос података о картици, потребних за плаћање. У овом случају понуда и избор апликација су шири, а укључује разне домаће и међународне апликације које су доступне на платформама за онлајн куповину и нису нужно уговорно повезане с одређеном банком.

Технички захтјеви укључују посједовање паметног мобилног уређаја са оперативним системом који подржава апликацију за мобилно плаћање коју желите да користите. С тим у вези, потребно је бити информисан прије одабира услуге. Поред наведеног, у већини случајева потребно је да мобилни уређај има стабилну интернет везу за вријеме коришћења апликације, а за chat банкарство и активну SIM картицу мобилног оператера.

2.4. Сигурносне функције и заштита од злоупотребе апликација за мобилно плаћање

Сигурност при плаћању и коришћењу апликација за мобилно плаћање је изузетно важна, те је у том смислу неопходно да сви ваши подаци, као и сваки приступ апликацији, буду заштићени од злоупотребе. Идентификација корисника приликом отварања апликације за плаћање и ауторизација плаћања врши се путем PIN-а или лозинке који су познати само кориснику или путем биометријских података корисника (отисак прста).

Изузетно је важно да запамтите свој PIN број и да га не дајете никоме.

За додатну заштиту, корисно је и закључавање екрана мобилног телефона другим кодом који је познат само кориснику телефона и који се разликује од PIN-а апликације, а корисник може подесити и коришћење биометријских података у сигурносне сврхе. Ако некоме позајмљујете мобилни телефон да обави позив или да нешто потражи, провјерите прије тога јесте ли се одјавили из апликација за плаћање или приступили својим рачунима/новцу. Никада не остављајте телефон без надзора.

Приликом одабира шифре или PIN-а, корисник треба избјегавати једноставне комбинације бројева (на примјер 1234, 1111, итд.) или рођендана, датума вјенчања итд. Увијек будите оригинални и креативни у одабиру лозинке или PIN-а.

Приликом одабира апликација за мобилно плаћање, посебно оних које захтијевају онлајн регистрацију и унос ваших података, као што су подаци о платним картицама, потребно је провјерити да ли је апликација на тржишту препозната као провјерена и сигурна, како користи ваше податке и да ли има све потребне елементе заштите. Преузмите оригиналне апликације искључиво из службених онлајн трговина.

2.5. Како функционишу бесконтактне платне картице и бесконтактне наруквице?

Бесконтактне платне картице омогућавају власнику такве картице плаћање на POS терминалима тако што ће платном картицом додирнути бесконтактни POS уређај. За износе веће од 60 КМ потребно је одобрити трансакцију PIN-ом картице. Бесконтактне платне картице раде на бази NFC технологије јер имају уграђен електронски чип који омогућава сигурну и брзу комуникацију са бесконтактним POS терминалом.

Наруквице за бесконтактно плаћање темеље се на истом принципу као и бесконтактне платне картице јер садрже мини картице које је потребно прислонити на бесконтактне POS терминале за плаћање. У случају већег износа, трансакција се одобрава уносом PIN-а.

2.6. Захтјеви за коришћење бесконтактних платних картица и наруквица

Услов за коришћење бесконтактне платне картице је отворен текући рачун у банци. Понуду је потребно прихватити подношењем захтјева и потписивањем уговора, било самостално било у оквиру одређеног пакета услуга.

Бесконтактна наруквица је у правилу везана за вашу платну картицу и припадајући рачун и уговара се као додатна мини картица.

2.7. Сигурносне карактеристике и заштита од злоупотребе бесконтактних платних картица и наруквица

Бесконтактне платне картице и наруквице треба чувати на сигурном и не давати другима. Тиме ће се власник заштитити од злоупотребе или неовлаштених трансакција. PIN за ауторизацију износа већег од 60 КМ мора се запамтити и никоме не саопштавати.

Важно је имати на уму да је свака трансакција заштићена посебном енкрипцијом и двоструко плаћање за исту куповину путем POS терминала није могуће, чак и ако се картица или наруквица тапну неколико пута.

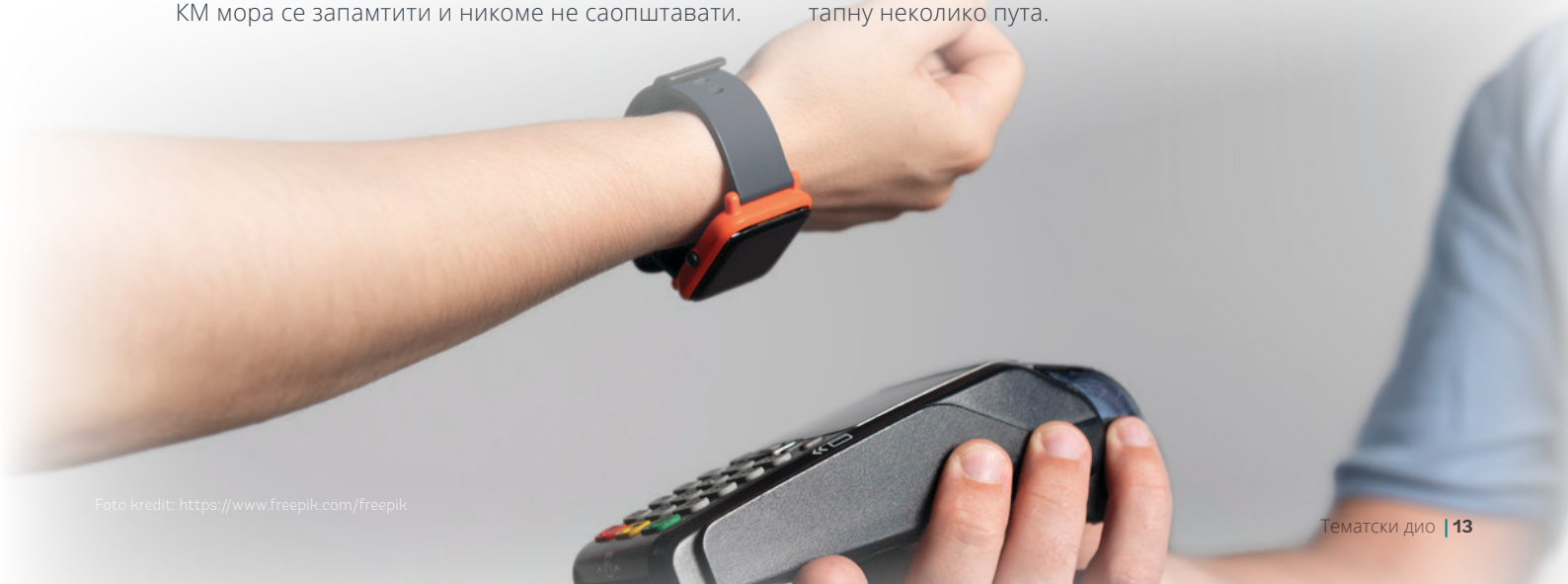
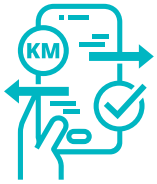


Foto kredit: https://www.freepik.com/freepik

Foto kredit: https://unsplash.com/@proxyclick

2.8. Основне обавезе за кориснике услуга дигиталног плаћања

Коришћење апликација за мобилно плаћање и бесконтактних платних картица и наруквица подразумијева прихватање одређених обавеза од стране корисника, првенствено ради заштите од могуће злоупотребе. У том смислу, осим што чувамо и не дијелимо своје кодове (PIN), потребно је имати на уму и да своје мобилне уређаје, картице или наруквице не дајемо другима. У случају губитка, банку треба одмах обавијестити како би се спријечила злоупотреба.



Неопходна је редовна провјера трансакција на рачуну, а ако примијетите трансакцију, чак и за минимални износ (нпр. 2 KM), коју нисте одобрили, као и све друге аномалије, одмах је пријавите својој банци.

Провјера детаља трансакције. Заправо, већина опција дигиталног плаћања заснована на апликацији омогућава двоструку верификацију како би корисник могао бити сигуран да је унио исправне податке о трансакцији (име и презиме примаоца, број рачуна, износ, сврха, итд.).

Остале обавезе укључују плаћање одређених накнада и провизија у складу са трошковима и условима понуде коју прихватате сваки пут када одаберете да користите услуге мобилне апликације, картице или наруквице.

Ако доступне информације о услузи нису довољно јасне, или не разумијете одређене термине који се користе у опису, важно је да прије коришћења тражите појашњење.

Ако нисте сигурни да је порука или имејл који сте примили упутио пружалац услуге (информације о услузи, комерцијалне понуде, обавијест о промјени капацитета услуге, итд.), немојте отварати такву поруку или имејл. Поготово ако порука садржи позив за достављање ваших личних података. У таквим случајевима, требали бисте код пружаоца услуге провјерити аутентичност поруке и њену сврху.

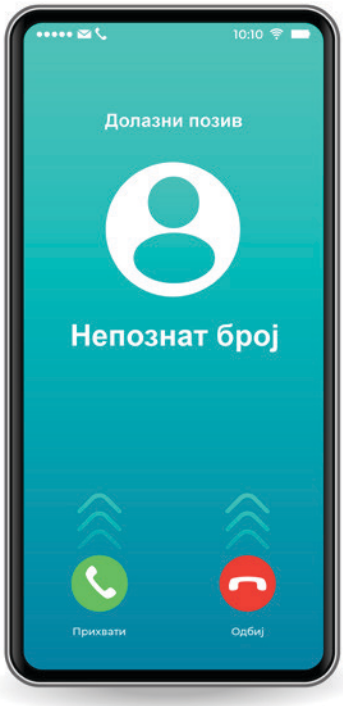
Добра је пракса увијек се распитати о понудама и условима прије одабира услуге. Ако понуда није довољно јасна и транспарентна, или прихватљива у смислу трошкова, требали бисте је избјегавати како бисте спријечили непредвиђене трошкове или другу штету.

2.9. Преварне или обмањујуће праксе којих корисници требају бити свјесни

Технолошки напредак и нове могућности које дају мобилне апликације, те бесконтактне платне картице и наруквице доносе и ризике у смислу могућих преварних или обмањујућих поступака. Важно је напоменути да се легитимна и провјерена употреба апликација континуирано ажурира најновијим софтверским рјешењима како би се понудио највиши ниво заштите од крађе података или преваре. Међутим, чак и уз ове заштите, важно је бити свјестан могућих превара и одговорности корисника приликом коришћења одређене апликације или линка, те приликом дијељења података. С тим у вези, најчешћи примјери преваре су социјални инжењеринг, односно када корисник својим дјеловањем омогући крађу података или превару. Неки примјери су наведени у наставку о phishingu, vishingu/гласовном phishingu и smishingu.

- **Phishing** укључује различите технике социјалног инжењеринга које се користе за крађу података од корисника финансијских услуга. Жртва се често контактира путем популарних друштвених мрежа са примамљивим понудама или линковима. Ова врста преваре може се појавити у облику атрактивних или примамљивих наслова, обећања, наизглед вјеродостојног садржаја који има за циљ навести корисника да кликне и успостави везу. Најчешће ови покушаји укључују vishing и smishing.

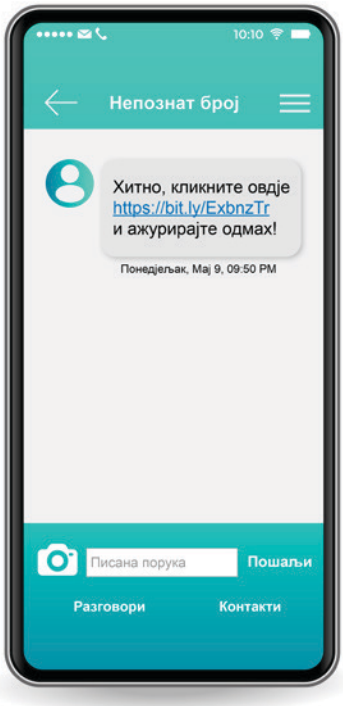
- **Vishing**, или гласовни phishing, дешава се када се жртва контактира путем телефона уз лажно представљање и од ње се траже подаци о платним картицама, банковним рачунима итд.



Примјер vishinga

Жртва користи бесконтактну платну картицу за свакодневне куповине. Једнога дана изненада добије позив са непознатог броја и особа која се представља као службеник банке хитно захтијева податке о картици за провјеру уплате од 100 КМ на основу награде коју је жртва освојила у банци.

- **Smishing**, или текстуални phishing, дешава се када се с непознатог броја пошаље SMS или порука из апликације за ћаскање са примамљивим садржајем који позива жртву да кликне на одређени линк. Отварањем линка прималац често невољно инсталира malware, односно штетну апликацију која може украсти његове личне податке с мобилног уређаја.

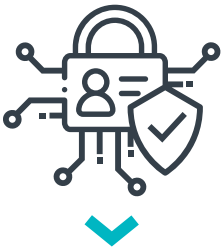


Примјер smishinga

Особа која користи апликацију за мобилно плаћање изненада добије SMS са непознатог броја да од сљедећег дана више неће радити апликација за плаћање инсталисана на његовом мобилном уређају и да одмах инсталише нову путем приложеног линка на SMS.

Осим ових примјера, постоје и друге преварне праксе које имају исти циљ да злоупотријебе податке корисника како би добили неовлаштени приступ и извршили незаконите трансакције. Још једна честа пракса преваре је скраћени URL, веб адреса, која често (иако не увијек) маскира злонамјерни URL намијењен омогућавању преваре. Зато је важно бити на опрезу. Важно је знати да су скраћени URL-ovi чести чак и код легитимне употребе, на примјер, друштвених медија (иако је у таквим случајевима могуће видјети и пуну адресу). Али у случајевима малициозне намјере, кориснику је тешко видјети пуну URL адресу (скривени подаци), па би коришћење ових адреса могло навести корисника да посјети лажне веб странице. Имајте на уму да увијек посјећујете легитимне веб странице. Сазнајте више о "сигурним опцијама" веб страница.

Важно је бити опрезан и увијек се придржавати основних сигурносних правила:



1. Користите антивирусни софтвер на свом паметном телефону
2. Редовно ажурирајте своје апликације
3. Инсталирајте само апликације из службене онлајн трговине
4. Запамтите и не дијелите своје приступне информације (лозинке, PIN, итд.)
5. Размислите о коришћењу потврде у 2 корака (тренутно већина водећих платформи и апликација нуди опцију верификације у 2 корака)
6. Будите информисани о опцијама токенизације (користећи токен за дигиталну идентификацију) или осигурајте своје трансакције верификацијом у 2 корака путем SMS-а
7. Не кликајте на садржај из непровјерених или сумњивих извора
8. Никада не дијелите податке о својој картици
9. Покријте тастатуру када уносите PIN у POS терминал
10. Редовно провјеравајте своје банковне изводе и одмах пријавите све неуобичајене трансакције вашој банци
11. Ако коришћење апликације или другог дигиталног начина плаћања укључује прихватање одредби и услова, прочитајте их прије прихватања и тражите појашњења гдје је потребно
12. Никада немојте користити уређаје с хакованим и/или илегално откључаним (rooted, JailBreaked, закрпљеним) OS или уређаје који су коришћени за приступ илегалним веб локацијама, као што су странице за дијељење торента, јер те странице често садрже злонамјерни код који може заразити ваш уређај и учинити га подложним хаковању и крађи личних података.

Ако корисник плаћања користи апликацију за плаћање на јавној мрежи или није сигуран у сигурносни ниво мреже за дијељење личних података, размислите о коришћењу енкрипције или коришћења виртуелне приватне мреже (VPN). Ако се користи VPN, препорука је да користите провјерени VPN који обично има претплату.

Арт Кредит: https://www.freepik.com/upklyak

2.10. Права потрошача - корисника, поступак приговора и надлежне институције за заштиту права потрошача

Коришћење опција дигиталног плаћања често је сигурно, али сигурност укључује усвајање одговорних пракси и понашања корисника. Ниво сигурности у процесу коришћења дигиталних плаћања пропорционалан је степену одговорности корисника услуга. Упркос будности корисника плаћања, понекад се дешавају преваре и обмане. Уколико дође до оваквих случајева, корисници плаћања треба да буду упознати са оквиром заштите права потрошача и како га користити.

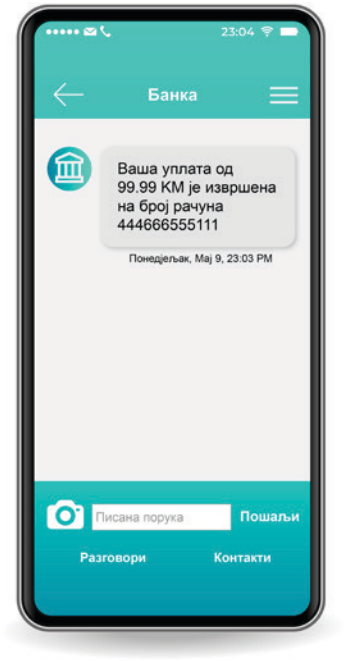
Кључни закони који регулишу правни оквир заштите потрошача су Закон о заштити корисника финансијских услуга ФБиХ, те Закони о банкама РС и ФБиХ. Ови закони прецизирају права и обавезе потрошача у свим фазама – од почетне фазе промоције и договарања платних услуга до завршне фазе потписаног уговора између пружаоца финансијских услуга и корисника плаћања. Закон такође наводи права и обавезе финансијских институција у погледу нивоа потребне транспарентности и сигурности информација. Закони прописују одредбе које уговори о банкарским услугама морају садржавати укључујући прецизне обавезе и права странака, детаље услуге, цијену и трајање услуга, начин обавјештавања и измјене уговора, поступке за раскид уговора, заштиту права и интереса корисника итд.

Препоручљиво је прочитати опште услове прије коришћења било које од опција дигиталног плаћања (или било којег другог финансијског производа или услуге). Закони у БиХ прописују обавезе финансијских институција када је у питању транспарентност услуга, што значи да свака услуга треба бити појашњена кроз уговор, али и друге документе. Требало би да прочитате уговор и другу документацију. Имате право да тражите појашњење услова и одредби. Одредбе које се односе на обавезе уговорних страна важне су за боље разумијевање које обавезе припадају вама, а које пружаоцу услуге.

Foto kredit: https://www.freepik.com/

Прво откривање злоупотребе

Први и најважнији корак је да одмах пријавите сваку злоупотребу или грешку вашој банци (нпр. трансакцију на вашем банковном изводу коју нисте одобрили, губитак платне картице или наруквице, сазнање да сте инсталирали апликацију која садржи злонамјерни софтвер, итд. Важно је пратити стање вашег рачуна, провјерити и пратити личне податке.



Банка ће подузети једностране, неопходне кораке да заштити ваш банковни рачун у зависности од врсте извјештаја. У пракси, то може укључивати блокирање ваше платне картице или наруквице, блокирање плаћања путем мобилног телефона или chata, двоструку провјеру начина на који је трансакција извршена и да ли је постојала ауторизација или друга радња која се сматра потребном у датој ситуацији.

Шта ако је приступ услузи привремено обустављен?

Да бисте повратили приступ дигиталним банкарским услугама, новој платној картици или наруквици, потребно је својој банци поднијети писмени извјештај/приговор. Писмени извјештај треба да садржи детаље трансакције (нпр. датум, име субјекта/лично име, износ трансакције, сумњу на злоупотребу података, итд.), затражити повратак средстава на ваш рачун (ако је било наплата или повлачења с вашег рачуна без вашег одобрења) као резултат пријављене злоупотребе. Корисник треба да води евиденцију комуникације између банке.

У складу са законским и подзаконским актима, банка ће прегледати уговор корисника и провјерити околности пријаве. Банка ће обавијестити корисника о подузетим корацима и извијестити о поднесеном извјештају/приговору.

Одмах пријавите злоупотребу или сумњиву трансакцију банци, или губитак картице или наруквице.

Банка ће подузети неопходне кораке да заштити ваш банковни рачун.

2.11. Омбудсмени за банкарски систем

Уколико корисник није задовољан одговором банке или није добио никакав одговор у року од 30 дана од писаног извјештаја/приговора, може се обратити омбудсмену за банкарски систем у надлежној ентитетској агенцији за банкарство. Важно је напоменути да се приговори омбудсмену за банкарски систем могу поднијети у року од шест мјесеци од дана пријема одговора пружаоца услуге или од истека рока од 30 дана који је прописан за одговор пружаоца услуга. Поступак је бесплатан.

Контакт подаци ентитетских омбудсмана за банкарски систем:

Агенција за банкарство Федерације БиХ

Омбудсмен за банкарски систем

Адреса: Змаја од Босне 47б,
71000 Сарајево

E-mail: ombudsmen@fba.ba

Телефон: 033 569 787

Агенција за банкарство Републике Српске

Омбудсмен за банкарски систем

Адреса: Васе Пелагића 11а,
78000 Бања Лука

E-mail: info@abrs.ba

Телефон: 051 224 079

По пријему приговора, у зависности од сваког појединачног случаја, омбудсмен ће анализирати да ли је приговор оправдан. Омбудсмен ће извршити увид у поступање банке и корисника, анализирати достављену документацију која показује временски оквир разговора између страна и размотрити оправданост рекламације. У зависности од добијених информација, омбудсмен одлучује да ли ће отворити случај. Ако омбудсмен одлучи да не отвори случај, тада ће савјетовати корисника да тражи даље поступање од друге релевантне институције. У зависности од ситуације, то може укључивати поновну комуникацију са пружаоцем финансијских услуга или заштиту права путем судског поступка. Ако омбудсмен отвори предмет, води поступак по приговору и даје препоруку банци. Одлука омбудсмена није правно обавезујућа.

Foto kredit: https://www.freepik.com/freepik

Важно је да приговор садржи потребне и прецизне податке о трансакцији, а уз приговор треба приложити одговарајућу документацију.

Приговор мора садржавати:

1. Име и презиме корисника
2. Поштанску адресу корисника и контакт телефон/имејл
3. Име и презиме, адресу и контакт телефон/имејл пуномоћника корисника (у случају да се рекламација шаље преко пуномоћника)
4. Пословни назив и адресу банке
5. Детаљне информације о спору између странака, када и гдје се то догодило
6. Сви примјењиви прилози (нпр. копија претходног приговора посланог банци, копија одговора банке, копија претходног приговора о банкарским услугама, други документи повезани са спором као што је пуномоћ, итд.)
7. Датум и мјесто вашег приговора
8. Потпис (у случају слања писма приговора)

Препоруке/мишљења омбудсмена нису обавезујуће (за разлику од судских одлука), али се могу користити као аргументи и битни су у даљим поступцима (било код финансијске институције било суда), посебно имајући у виду да омбудсмен за банкарство дјелује у оквиру Агенције за банкарство као регулатор комерцијалног финансијског тржишта.

2.12. Посредовање као могућност вансудског поравнања

Алтернативно, ако се стране слажу, препорука може укључивати покретање поступка посредовања код омбудсмена за банкарски систем како би се тражило рјешење. У циљу рјешавања питања и заштите права, странке се могу договорити да покрену поступак посредовања код омбудсмена за банкарски систем и да на тај начин траже рјешење.

Посредовање је једна од могућности вансудског поравнања. Предност поступка посредовања је у томе што је флексибилнији, једноставнији и јефтинији од судског поступка. Важно је истаћи да је за покретање поступка неопходна сагласност обје стране и да се поступак не може покренути једнострано. Током посредовања медијатор (омбудсмен) не може наметати рјешења, али може олакшати комуникацију и пружити стручне савјете како би помогао странкама да нађу рјешење.

- Посредовање је добровољни поступак који није правно обавезујући, али је флексибилнији и јефтинији од судског поступка
- Странке заједнички подносе захтјев за покретање поступка посредовања. Није могуће поднијети захтјев једнострано
- Захтјев се подноси у писаној форми
- Посредник не намеће рјешења, али она могу помоћи у олакшавању комуникације и савјетима
- Сама процедура поредовања је бесплатна

Уколико омбудсмен није надлежан за дати приговор, може савјетовати корисника да тражи даље поступање код других релевантних институција и које кораке треба да подузме.

С обзиром на то да се дигитална плаћања често врше за куповину робе и услуга, спорови и рекламације се понекад не односе на пружаоца дигиталних услуга, већ на трговца који продаје робу или услуге. У таквим случајевима примјењују се општа правила заштите потрошача. У Босни и Херцеговини куповина, онлајн куповина или куповина на даљину регулисана је законима о заштити потрошача и у надлежности је омбудсмена за заштиту потрошача БиХ. Више о институцији омбудсмена за заштиту потрошача у БиХ можете сазнати на www.ozp.gov.ba. Жалбе се могу поднијети директно или путем службене веб странице.

Заштита права се може остварити и путем суда. Правосудни систем у БиХ, у зависности од природе захтјева или повреде права, пружа заштиту у различитим поступцима. Корисно је, у случају тражења заштите права преко суда, консултовати се и тражити стручну правну помоћ.


Foto kredit: https://www.freepik.com/pressfoto
CONTRACT

Упитник за читаоце да процијене своје знање

Имајте на уму да је на свако питање могућ само један тачан одговор

1 **Која је главна карактеристика безготовинског плаћања?**

а) Трансакција се одвија без физичког трансфера новца

б) Трансакција се одвија кредитном картицом

ц) Трансакција се одвија само за куповину путем интернета

2 **Ствари које не можете учинити с апликацијом за мобилно банкарство?**

а) Провјерити стање на рачуну

б) Направити налог за плаћање

ц) Потписати уговор

3 **Бесконтактне платне картице функционишу на основу које технологије?**

а) NFC

б) DFC

ц) FNC

4 **Ради ваше сигурности, изузетно је важно да:**

а) Запамтите свој PIN број и подијелите га са неким блиским пријатељима (за помоћ у случају да се не можете сјетити)

б) Заштитите све своје податке, као и сваки приступ апликацији, од злоупотребе коришћењем PIN-а или лозинке и биометрије

ц) Приликом одабира шифре или PIN-а, користите једноставне комбинације бројева како бисте апликацију учинили лакшом за коришћење

5 **Који су најчешћи примјери преваре?**

а) Vishing

б) Позивање

ц) Ћаскање

6 **Ако примијетите неуобичајену трансакцију, злоупотребу или грешку апликације за мобилно плаћање, прво што требате учинити је да:**

а) Редовно ажурирате своју апликацију за мобилно плаћање

б) Одмах пријавите сваку злоупотребу или грешку вашој банци дајући потребне информације

ц) Контактирате примаоца трансакције и затражите појашњење

7 **Који закони регулишу заштиту потрошача финансијских услуга у ентитетима?**

а) Закон о финансијским институцијама у Федерацији БиХ и Републици Српској

б) Закон о заштити корисника финансијских услуга Федерације БиХ и Закон о банкама Републике Српске

ц) Закон о заштити потрошача финансијских средстава у Федерацији БиХ и Републици Српској

8 **Која је улога омбудсмена за банкарски систем?**

а) Штити људска и радна права запослених у финансијским институцијама

б) Штити права и интересе банака

ц) Штити права и интересе корисника финансијских услуга и производа

9 **Корисник финансијских услуга може упутити писмени приговор омбудсмену за банкарски систем у надлежној ентитетској агенцији за банкарство.**

а) Уколико корисник није задовољан одговором пружаоца услуге или није добио никакав одговор у року од 30 дана од писаног извјештаја

б) Ако корисник нема повјерења у пружаоца услуга и уопште не жели комуникацију

ц) Ако је корисник за плаћање користио нерегулисану услугу

10 **Приговор омбудсмену за банкарски систем може се поднијети у року:**

а) дванаест мјесеци од датума пријема одговора пружаоца услуга

б) девет мјесеци од дана пријема одговора пружаоца услуга

ц) шест мјесеци од дана пријема одговора пружаоца услуга

11 **Коју опцију нуди омбудсмен за банкарски систем као вансудско решење спора?**

а) Посредовање

б) Помирење

ц) Заступање пред судом

12 **Закони (који садрже норме о заштити потрошача - корисника финансијских услуга/производа) у БиХ прописују обавезе финансијских институција када је у питању:**

а) Распон цијена услуга дигиталног плаћања

б) Транспарентност услуге и права и обавезе потрошача у свим фазама

ц) Коришћење верификације у 2 корака на апликацијама за мобилно плаћање

Списак тачних одговора из упитника

Питање	Тачан одговор	Питање	Тачан одговор
1	А	7	Б
2	Ц	8	Ц
3	А	9	А
4	Б	10	Ц
5	А	11	А
6	Б	12	Б

Рјечник основних појмова коришћених у Водичу

ATM

Банкомат (ATM) је електронска банка која омогућава клијентима да заврше основне трансакције без помоћи представника филијале или благајника. Свако ко има кредитну или дебитну картицу може приступити готовини на већини банкомата.

Банковни рачун

Банковни рачун је финансијска услуга/производ. То је рачун који води банка и користи се за плаћања и депозите. Свака финансијска институција (банка) поставља услове за сваку врсту рачуна који нуди.

Бесконтактно плаћање

Бесконтактне платне картице омогућавају власнику такве картице да врши плаћања на POS терминалима додиром платне картице на бесконтактни POS уређај. Наруквице за бесконтактно плаћање темеље се на истом принципу као и бесконтактне платне картице јер садрже мини картице које је потребно прислонити на бесконтактне POS терминале за плаћање.

Дебитна картица

Дебитна картица је повезана са текућим банковним рачуном. Средства која су доступна на рачуну троше се дебитном картицом.

Дигиталне финансијске услуге

Финансијске услуге подржане модерним технологијама и које се нуде путем мобилних телефона, POS уређаја и интернета. Услуге које се нуде дигитално могу драматично смањити трошкове за купце и пружаоце услуга.

Права заштите потрошача финансијских услуга

Права заштите потрошача финансијских услуга прописана су низом закона и прописа које доносе регулаторне институције и представљају правни оквир за заштиту корисника финансијских производа и услуга.

Финансијска институција/пружалац финансијских услуга

Финансијска институција је друштво које се бави пружањем финансијских услуга и производа и финансијским и монетарним трансакцијама као што су депозити, кредити, плаћања, инвестиције и мијењање валута. У Босни и Херцеговини најчешће финансијске институције на тржишту су банке, микрокредитне организације и лизинг компаније.

Превара

Превара је поступак обмане у којој је једну особу финансијски преварила друга особа. Постоји много различитих врста превара у финансијама или банкарству. Неке од најчешћих врста превара су превара с дебитним и кредитним картицама, крађа идентитета, превара у дигиталном плаћању, превара у сефовима итд.

Malware

Malware (скраћено од "злонамјерни софтвер" (енг. malicious software)) је датотека или код (испоручен преко мреже), осмишљен тако да поремети, оштети, украде или добије неовлаштени приступ рачунарском систему.

Посредовање

Посредовање је једно од могућности вансудског рјешавања спора. Предност поступка посредовања је што је флексибилнији, једноставнији и јефтинији од судског поступка.

Мобилна апликација

Мобилна апликација или app је софтверска апликација или рачунарски програм дизајниран за рад на мобилном уређају као што је паметни телефон, таблет или паметни сат.

Мобилно банкарство

Мобилно банкарство користи мобилне телефоне као канал за пружање финансијских услуга. Мобилно банкарство подржава платне трансакције укључујући трансфере новца, текуће рачуне, а у неким случајевима и отплату кредита, лично планирање итд.

Мобилно плаћање

Мобилно плаћање је финансијска трансакција извршена путем мобилног уређаја или другог преносног електронског уређаја. То је финансијски производ или услуга. Мобилно плаћање је финансијска услуга и производ и може се користити и за слање новца другима.

NFC (комуникација блиског поља)

Комуникација блиског поља (NFC) је скуп комуникацијских протокола који омогућава комуникацију између два електронска уређаја на одређеној удаљености (од 4 цм или мање).

Омбудсмени за банкарски систем у Босни и Херцеговини

Омбудсмен за банкарски систем је институција основана на ентитетском нивоу ради промоције и заштите права и интереса грађана као корисника финансијских услуга. Постоје различити механизми за заштиту права, као што су рекламацијски поступак или посредовање.

Одобрење плаћања

Одобрење плаћања је процес који верификацијом чини плаћање сигурнијим. Идентификација корисника приликом отварања апликације за плаћање и одобрење плаћања проводе се путем PIN-а или лозинке који је познат само кориснику, или путем биометријских података корисника (отисак прста и/или скенирање мрежнице).

Лозинка

Лозинка је нумерички низ који се користи за потврђивање идентитета корисника на рачунару или другом електронском уређају.

Phishing

Phishing је превара као пракса сајбер напада који се често користи за крађу корисничких података, укључујући податке за пријаву и бројеве кредитних картица. Најчешћа пракса напада је када је прималац преварен да кликне на злонамјерни линк.

PIN

Лични идентификациони број (PIN) је нумерички код који се користи као механизам идентификације, углавном у електронским финансијским трансакцијама. Лични идентификациони бројеви се обично издају у вези са платним картицама, мобилним банкарством, те разним облицима дигиталног плаћања и могу бити потребни за довршетак трансакције.

Уређај на продајном мјесту (POS)

Мали, преносиви уређај који олакшава електронску финансијску трансакцију. POS уређаји у одређеним случајевима могу послужити и као мјесто банкарског пословања. Овај уређај се користи у трговању и куповини приликом безготовинског плаћања разних роба и услуга. Будући да су јефтини и лако преносиви, играју важну улогу у премошћавању локацијског јаза и омогућавању приступа финансијским услугама у руралним подручјима и подручјима са неразвијеном инфраструктуром.

QR код

Брзи одговор или QR код је дводимензионална верзија баркода, која се обично састоји од црних и бијелих узорака пиксела. QR код садржи одређене информације (различитих типова) које софтвер може лако прочитати. QR код олакшава провођење процеса плаћања итд.

SMS (услуга кратких порука)

Услуга кратких порука или SMS је технологија за слање кратких текстуалних порука између мобилних телефона. SMS се често користи за верификацију (коришћење услуга, плаћања, итд.).

Vishing

Vishing је пракса преваре, комбинација 'гласа' и 'phishinga'. То је телефонска превара или гласовна порука дизајнирана да наведе корисника да подијели личне податке.

VPN (виртуелна-приватна-мрежа)

Виртуелна приватна мрежа или VPN је шифрована веза између уређаја и интернет мреже. Главна сврха VPN-а је успостављање заштићене мрежне везе приликом коришћења јавних мрежа и помаже у заштити преноса података.

Приједлог корисних линкова

Корисни линкови институција

Централна банка Босне и Херцеговине: www.cbbh.ba

Централна банка Босне и Херцеговине - веб страница о финансијској едукацији: fined.cbbh.ba

Агенција за банкарство Федерације БиХ / Омбудсмени за банкарски систем:

www.fba.ba; www.fba.ba/bs/ombudsmen-18

www.fba.ba/objection-form/1760

E-mail: ombudsman@fba.ba

Агенција за банкарство Републике Српске / Омбудсмени за банкарски систем:

www.abrs.ba; www.abrs.ba/sr/ombdsman/c90;

E-mail: info@abrs.ba

Пратите нас:

www.cbbh.ba

Twitter: @CBBiH

YouTube канал: Централна банка Босне и Херцеговине

Facebook: www.facebook.com/CentralnaBankaBiH

LinkedIn: www.linkedin.com/company/cbbih

Централна банка Босне и Херцеговине

Служба за односе са јавношћу

pr@cbbh.ba

contact@cbbh.ba

+387 (33) 278 123

+387 (33) 201 517

Свјетска банка

E-mail: bih@worldbank.org

Телефон: +387 (33) 251 500

Web: www.worldbank.org/en/country/bosniaandherzegovina

Facebook: @WorldBankBiH

Арт-Кредит: https://www.freepik.com/freepik

Centralna banka
BOSNE I HERCEGOVINE

Централна банка
БОСНЕ И ХЕРЦЕГОВИНЕ

WORLD BANK GROUP
Finance, Competitiveness & Innovation