



Vodič za digitalna plaćanja

MAJ 2022



Centralna banka
BOSNE I HERCEGOVINE

Централна банка
БОСНЕ И ХЕРЦЕГОВИНЕ



WORLD BANK GROUP
Finance, Competitiveness & Innovation



Odricanje od odgovornosti

Ovaj rad je proizvod osoblja Svjetske banke uz vanjske doprinose Centralne banke Bosne i Hercegovine i njenih saradnika. Nalazi, tumačenja i zaključci izraženi u ovom radu ne odražavaju nužno stavove Svjetske banke, njenog Odbora izvršnih direktora ili vlada koje oni predstavljaju. Sadržaj, tumačenja i zaključci ne predstavljaju nužno stavove Centralne banke Bosne i Hercegovine i njenog Upravnog vijeća. Svjetska banka ne garantuje tačnost podataka uključenih u ovaj rad. Granice, boje, denominacije i druge informacije prikazane na bilo kojoj karti u ovom radu ne podrazumijevaju bilo kakvu prosudbu Svjetske banke u vezi sa pravnim statusom bilo koje teritorije ili odobravanjem ili prihvatanjem takvih granica.

Prava i dozvole

Materijal u ovom radu podliježe autorskim pravima. Budući da Svjetska banka podstiče širenje svog znanja, ovo djelo se može umnožavati, u cjelini ili djelimično, u nekomercijalne svrhe, sve dok se uključi potpuno pripisivanje materijala ovom radu.

SADRŽAJ

1. UVOD	5
2. TEMATSKI DIO – Vrste digitalnih plaćanja i zaštita prava potrošača	7
2.1. Različiti pristupi digitalnom plaćanju u BiH	7
2.2. Šta su aplikacije za mobilno plaćanje?	8
2.3. Aktivacija i tehnički uslovi za korištenje aplikacija za mobilno plaćanje	12
2.4. Sigurnosne funkcije i zaštita od zloupotrebe aplikacija za mobilno plaćanje	12
2.5. Kako funkcioniraju beskontaktno platne kartice i beskontaktno narukvice?	13
2.6. Zahtjevi za korištenje beskontaktnih platnih kartica i narukvica	13
2.7. Sigurnosne karakteristike i zaštita od zloupotrebe beskontaktnih platnih kartica i narukvica	13
2.8. Osnovne obaveze za korisnike usluga digitalnog plaćanja	15
2.9. Prevarne ili obmanjujuće prakse kojih korisnici trebaju biti svjesni	16
2.10. Prava potrošača - korisnika, postupak prigovora i nadležne institucije za zaštitu prava potrošača	20
2.11. Ombudsmeni za bankarski sistem	22
2.12. Posredovanje kao mogućnost vansudskog poravnanja	24
Upitnik za čitaoce da procijene svoje znanje	26
Rječnik osnovnih pojmova korištenih u Vodiču	28
Prijedlog korisnih linkova	30



1. UVOD

Razvojem i tehnološkim napretkom društva javljaju se nove potrebe finansijskih korisnika i stvaraju novi izazovi na finansijskom tržištu. Jedan od novijih događaja je pojava novih opcija plaćanja za obavljanje finansijskih transakcija. Pored klasičnog gotovinskog plaćanja, uz podršku savremenih tehnologija razvijaju se i različiti oblici digitalnog, bezgotovinskog plaćanja. Pandemija COVID-19 učinila je digitalno plaćanje još praktičnijim u odnosu na tradicionalne načine plaćanja, prvenstveno zbog mogućnosti smanjenja prenosa virusa. S obzirom na dalji razvoj tehnologije, očekuje se da će ovi načini plaćanja i transfera novca povećati svoj udio u ukupnim plaćanjima.

U ovom vodiču ćemo se fokusirati na najnovije trendove u digitalnom, bezgotovinskom plaćanju dostupnom građanima u Bosni i Hercegovini. Na tržištu su sve češće različite vrste bezgotovinskog plaćanja, a dinamika i brzina razvoja nameću potrebu za povećanjem edukacije i svijesti javnosti kako bi se bezgotovinsko plaćanje moglo odgovornije i sigurnije koristiti.

Digitalna plaćanja su bezgotovinske transakcije, odnosno plaćanja roba i usluga koja se odvijaju isključivo u datom elektronskom/virtualnom okruženju.

Glavna karakteristika bezgotovinskog plaćanja je da se transakcija odvija bez fizičkog transfera novca. To znači da i platilac (osoba koja plaća) i primalac plaćanja (primalac koji prima novac) nemaju kontakt sa gotovinom. Prednost digitalnog plaćanja ogleda se u tome što platilac može izvršiti plaćanje u bilo koje vrijeme, bez obzira na lokaciju, na brz i jednostavan način, koristeći odabrana tehnološka rješenja (npr. posebnu mobilnu aplikaciju ili cijeli paket usluga – mobilno i/ili internet bankarstvo).

Digitalizacija usluga zahtijeva edukaciju korisnika finansijskih plaćanja kako bi mogli na siguran i odgovoran način koristiti savremene platne usluge. Jednako je važno educirati potrošače o njihovim pravima i mogućnostima za otklanjanje potencijalne zloupotrebe i slučajeva prevare u vezi s digitalnim plaćanjem. U tom smislu, u nastavku će se detaljnije govoriti o najnovijim tržišnim trendovima vezanim za mobilno i beskontaktno plaćanje i njegovim karakteristikama, uključujući različite pristupe digitalnom plaćanju u BiH, osnovne vrste digitalnog plaćanja, tehničke zahtjeve i obaveze korisnika, kao i informacije o lažnim ili obmanjujućim praksama kojih bi korisnici plaćanja trebali biti svjesni. Takođe, vodič će ponuditi informacije o pravima potrošača, objasniti procedure za podnošenje prigovora, te navesti nadležne bh. institucije za zaštitu prava potrošača.



2. TEMATSKI DIO – Vrste digitalnih plaćanja i zaštita prava potrošača

2.1. Različiti pristupi digitalnom plaćanju u BiH

U Bosni i Hercegovini su dostupni različiti modeli, inovativni pristupi i usluge za digitalno plaćanje. Sve banke u BiH izdaju platne kartice za plaćanja (kontaktna i beskontaktna) preko Point-of-Service (POS) terminala i putem interneta (u fizičkom i online okruženju). Međutim, na tržištu su sve prisutnije druge mogućnosti. Osnovna podjela se može napraviti između aplikacija (apps) koje su razvile komercijalne finansijske institucije poput banaka i onih koje služe kao sredstvo za plaćanje usluga drugih kompanija za kupovinu ili pružene usluge. Sveukupno, cilj je omogućiti jednostavnije, sigurnije i brže plaćanje, a značaj se pridaje i ekološkim prednostima kroz smanjenje upotrebe papira ili drugih materijalnih resursa. Aplikacije posebnu pažnju posvećuju plaćanju i sigurnosti pohrane podataka, pa je važno biti svjestan rješenja koja aplikacije nude i da li ona odgovaraju nečijim potrebama plaćanja.

Na primjer, neke kompanije nude posebnu aplikaciju za plaćanje svojih usluga koja je povezana sa računom kod banke partnera; korisnik preuzima aplikaciju sa popularnih servisa, registruje se (sa podacima o kartici, određenim ličnim podacima i referentnim brojem usluge) i otvara račun u banci kako bi aplikacija ostala aktivna. Proces plaćanja se uglavnom odvija kroz periodično kreirane naloge (obavještenja o dospjeću plaćanja) i nema potrebe za odlaskom u banku ili ponovnim unosom podataka za plaćanje. Uobičajena je praksa da određena aplikacija dozvoljava plaćanja višestrukim pružaocima usluga. Finansijske institucije pružaju svojim klijentima i različite opcije digitalnog plaćanja, stalno ažuriraju svoju praksu, pomažu u evidentiranju transakcija i olakšavaju njihovu upotrebu (na primjer, dodatni mehanizmi zaštite koji pokrivaju proces plaćanja bez potrebe za potvrđivanjem potencijalno rizičnih transakcija ili metoda skladištenja podataka posebnim pozivima - tokenizirani pristup ili opcija za upravljanje ličnim finansijama pomoću alata za obračun troškova itd.).

Opcije digitalnog plaćanja provjerite kod svog finansijskog ili drugog pružaoca usluga. Lakoća ili složenost korištenja, brzina, dodatne mogućnosti plaćanja, niži troškovi za ovu vrstu plaćanja, da li je aplikacija dostupna pod uslovom otvaranja računa u posebnoj banci ili je vezana za drugu vrstu usluge itd. važna su pitanja o kojima treba razmišljati i tražiti odgovore prije nego što donesete odluku o korištenju digitalnog plaćanja.

2.2. Šta su aplikacije za mobilno plaćanje?

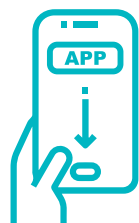
Aplikacije za mobilno plaćanje (apps) su posebni softverski programi kreirani za pametne telefone ili tablete, koji korisnicima omogućavaju različite vrste plaćanja. Osim funkcionalnosti plaćanja, ove aplikacije često omogućavaju i druge funkcionalnosti kao što su: provjera stanja na računu, pregled troškova, podnošenje online aplikacija, marketing i učešće u promotivnim kampanjama, komunikacija s pružaocima finansijskih usluga između ostalih funkcionalnosti korisnika.

Na tržištu postoje različite vrste, a razlikuju se po načinu na koji pružaju usluge platnog prometa. Postoji nekoliko opcija plaćanja, a najčešće su:





i) **Plaćanje putem elektronskog naloga za plaćanje** vrši se instaliranjem i pokretanjem aplikacije i početnim unosom dodijeljenog PIN-a ili biometrijskih podataka (obično otiska prsta). Aplikacije za plaćanje već sadrže softverski definirane elemente naloga za plaćanje koje je potrebno popuniti zavisno od vrste plaćanja. Time se olakšava korištenje usluge. Najvažniji elementi naloga (koji je izabrao i/ili popunio korisnik) su izbor računa sa kojeg se vrši plaćanje (samo ako imate više naloga), svrha plaćanja, podaci o primaocu uplate (naziv/ime i adresa), račun primaoca uplate i iznos uplate. Dodatni elementi biće potrebni samo u slučaju međunarodnih plaćanja ili plaćanja javnih prihoda. Kreirani nalog se potvrđuje ponovnim unosom PIN-a ili biometrije, nakon čega se plaćanje smatra obavljenim.



Instalacija aplikacije



Pokretanje aplikacije PIN-om ili biometrijskim podacima



Popunjavanje naloga za plaćanje



Odobriti plaćanje PIN-om ili biometrijskim podacima



ii) **Aplikacije sa mogućnošću očitavanja Quick Response (QR) kodova** koji se nalaze na fakturama prodavca koji dozvoljavaju ovu vrstu plaćanja. Nakon pokretanja aplikacije potrebno je odabrati opciju plaćanja, skenirati QR kod računa mobilnim uređajem, te odobriti plaćanje PIN-om ili biometrijskim podacima, nakon čega se plaćanje smatra obavljenim.



Pokretanje aplikacije



Odabrati opciju plaćanja QR kodom



Skenirati QR kod računa



Odobriti plaćanje PIN-om ili biometrijskim podacima



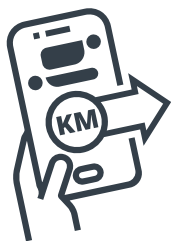
iii) **Plaćanje putem tehnologije komunikacije bliskog polja (NFC).** Ova opcija znači da aktivirate ovu funkcionalnost unutar postojeće aplikacije za mobilno plaćanje (kao što je aplikacija za mobilno bankarstvo) ili unosom drugih potrebnih podataka poput onih koji se odnose na vašu platnu karticu, uz obaveznu aktivaciju NFC opcije u postavkama mobilnog uređaja. Plaćanje vršite otključavanjem mobilnog telefona i stavljanjem zadnje strane mobilnog uređaja na beskontaktni POS terminal, bez obzira na to imate li internet konekciju ili ne. Važno je napomenuti da aplikaciju nije potrebno pokretati, ali da biste izvršili plaćanje obično je potrebno unijeti PIN kartice na POS terminalu. Na taj način je omogućeno plaćanje bez platne kartice pri ruci.



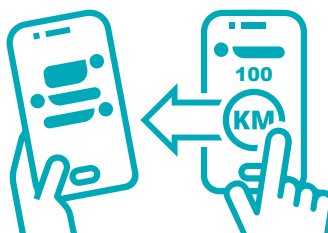
Otključavanje
mobilnog telefona



Stavljanje mobilnog
uređaja na
beskontaktni POS
terminal



iv) **Chat aplikacije** se mogu prilagoditi i za funkcionalnost plaćanja. Trenutno se najčešće koriste za provjeru stanja na računu, slanje novca osobama u vašem imeniku koje su se registrovale za primanje novca putem te aplikacije i plaćanje unaprijed definisanih računa (na primjer, komunalije, struja, plin, itd.). Iznosi transakcija su ograničeni (na primjer na 200 KM), aktivacija je često povezana s drugom postojećom digitalnom uslugom (kao što je mobilno bankarstvo) i svako plaćanje se provjerava unosom odgovarajućeg PIN-a





2.3. Aktivacija i tehnički uslovi za korištenje aplikacija za mobilno plaćanje

Plaćanje se obično vrši povezivanjem aplikacije sa vašim bankovnim računom ili platnom karticom. Aktivacija aplikacije koja je povezana s vašim bankovnim računom obično zahtijeva postojanje ugovornog odnosa između banke i vlasnika računa uz prihvatanje uslova korištenja, bilo kao pojedinačne usluge bilo usluge u okviru određenog paketa usluga. Takve aplikacije uključuju aplikacije za mobilno bankarstvo, aplikacije za chat bankarstvo i druge specijalizovane bankarske aplikacije.

Aktivacija aplikacije koja je povezana s platnom karticom obično podrazumijeva online registraciju korisnika, uz prihvatanje uslova korištenja i početni unos podataka o kartici, potrebnih za plaćanje. U ovom slučaju ponuda

i izbor aplikacija su širi, a uključuje razne domaće i međunarodne aplikacije koje su dostupne na platformama za online kupovinu i nisu nužno ugovorno povezane s određenom bankom.

Tehnički zahtjevi uključuju posjedovanje pametnog mobilnog uređaja sa operativnim sistemom koji podržava aplikaciju za mobilno plaćanje koju želite da koristite. S tim u vezi, potrebno je biti informisan prije odabira usluge. Pored navedenog, u većini slučajeva potrebno je da mobilni uređaj ima stabilnu internet vezu za vrijeme korištenja aplikacije, a za chat bankarstvo i aktivnu SIM karticu mobilnog operatera.

2.4. Sigurnosne funkcije i zaštita od zloupotrebe aplikacija za mobilno plaćanje

Sigurnost pri plaćanju i korištenju aplikacija za mobilno plaćanje je izuzetno važna, te je u tom smislu neophodno da svi vaši podaci, kao i svaki pristup aplikaciji, budu zaštićeni od zloupotrebe. Identifikacija korisnika prilikom otvaranja aplikacije za plaćanje i autorizacija plaćanja vrši se putem PIN-a ili lozinke koji su poznati samo korisniku ili putem biometrijskih podataka korisnika (otisak prsta).

Za dodatnu zaštitu, korisno je i zaključavanje ekrana mobilnog telefona drugim kodom koji je poznat samo korisniku telefona i koji se razlikuje od PIN-a aplikacije, a korisnik može podesiti i korištenje biometrijskih podataka u sigurnosne svrhe. Ako nekome pozajmljujete mobilni telefon da obavi poziv ili da nešto potraži, provjerite prije toga jeste li se odjavili iz aplikacija za plaćanje ili pristupili svojim računima/novcu. Nikada ne ostavljajte telefon bez nadzora.

Prilikom odabira šifre ili PIN-a, korisnik treba izbjegavati jednostavne kombinacije brojeva (na primjer 1234, 1111, itd.) ili rođendana, datuma vjenčanja itd. Uvijek budite originalni i kreativni u odabiru lozinke ili PIN-a.

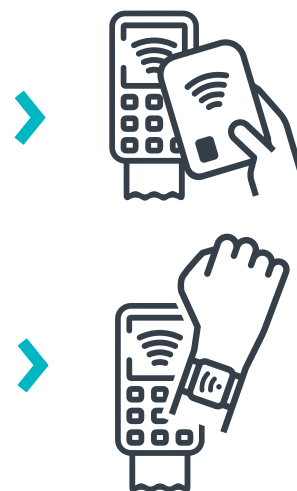
Izuzetno je važno da zapamtite svoj PIN broj i da ga ne dajete nikome.

Prilikom odabira aplikacija za mobilno plaćanje, posebno onih koje zahtijevaju online registraciju i unos vaših podataka, kao što su podaci o platnim karticama, potrebno je provjeriti da li je aplikacija na tržištu prepoznata kao provjerena i sigurna, kako koristi vaše podatke i da li ima sve potrebne elemente zaštite. Preuzmite originalne aplikacije isključivo iz službenih online trgovina.

2.5. Kako funkcioniraju beskontaktno platne kartice i beskontaktno narukvice?

Beskontaktno platne kartice omogućavaju vlasniku takve kartice plaćanje na POS terminalima tako što će platnom karticom dodirnuti beskontaktni POS uređaj. Za iznose veće od 60 KM potrebno je odobriti transakciju PIN-om kartice. Beskontaktno platne kartice rade na bazi NFC tehnologije jer imaju ugrađen elektronski čip koji omogućava sigurnu i brzu komunikaciju sa beskontaktnim POS terminalom.

Narukvice za beskontaktno plaćanje temelje se na istom principu kao i beskontaktno platne kartice jer sadrže mini kartice koje je potrebno prisloniti na beskontaktno POS terminale za plaćanje. U slučaju većeg iznosa, transakcija se odobrava unosom PIN-a.



2.6. Zahtjevi za korištenje beskontaktnih platnih kartica i narukvica

Uslov za korištenje beskontaktno platne kartice je otvoren tekući račun u banci. Ponudu je potrebno prihvatiti podnošenjem zahtjeva i potpisivanjem ugovora, bilo samostalno bilo u okviru određenog paketa usluga.

Beskontaktna narukvica je u pravilu vezana za vašu platnu karticu i pripadajući račun i ugovara se kao dodatna mini kartica.

2.7. Sigurnosne karakteristike i zaštita od zloupotrebe beskontaktnih platnih kartica i narukvica

Beskontaktno platne kartice i narukvice treba čuvati na sigurnom i ne davati drugima. Time će se vlasnik zaštititi od zloupotrebe ili neovlaštenih transakcija. PIN za autorizaciju iznosa većeg od 60 KM mora se zapamtiti i nikome ne saopštavati.

Važno je imati na umu da je svaka transakcija zaštićena posebnom enkripcijom i dvostruko plaćanje za istu kupovinu putem POS terminala nije moguće, čak i ako se kartica ili narukvica tapnu nekoliko puta.





Scan your badge or Facebook code

sunix

Hold your code 10-15 cm from the camera



Hold your code 10-15 cm from the camera

Code not recognized

MALA SWITZERLAND

TO LOND BY JET

ALL AMERICA

2.8. Osnovne obaveze za korisnike usluga digitalnog plaćanja

Korištenje aplikacija za mobilno plaćanje i beskontaktnih platnih kartica i narukvica podrazumijeva prihvatanje određenih obaveza od strane korisnika, prvenstveno radi zaštite od moguće zloupotrebe. U tom smislu, osim što čuvamo i ne dijelimo svoje kodove (PIN), potrebno je imati na umu i da svoje mobilne uređaje, kartice ili narukvice ne dajemo drugima. U slučaju gubitka, banku treba odmah obavijestiti kako bi se spriječila zloupotreba.



Neophodna je redovna provjera transakcija na računu, a ako primijetite transakciju, čak i za minimalni iznos (npr. 2 KM), koju niste odobrili, kao i sve druge anomalije, odmah je prijavite svojoj banci.



Provjera detalja transakcije. Zapravo, većina opcija digitalnog plaćanja zasnovana na aplikaciji omogućava dvostruku verifikaciju kako bi korisnik mogao biti siguran da je unio ispravne podatke o transakciji (ime i prezime primaoca, broj računa, iznos, svrha, itd.).



Ostale obaveze uključuju plaćanje određenih naknada i provizija u skladu sa troškovima i uslovima ponude koju prihvatate svaki put kada odaberete da koristite usluge mobilne aplikacije, kartice ili narukvice.



Ako dostupne informacije o usluzi nisu dovoljno jasne, ili ne razumijete određene termine koji se koriste u opisu, važno je da prije korištenja tražite pojašnjenje.



Ako niste sigurni da je poruka ili e-mail koji ste primili uputio pružalac usluge (informacije o usluzi, komercijalne ponude, obavijest o promjeni kapaciteta usluge, itd.), nemojte otvarati takvu poruku ili e-mail. Pogotovo ako poruka sadrži poziv za dostavljanje vaših ličnih podataka. U takvim slučajevima, trebali biste kod pružaoca usluge provjeriti autentičnost poruke i njenu svrhu.

Dobra je praksa uvijek se raspitati o ponudama i uslovima prije odabira usluge. Ako ponuda nije dovoljno jasna i transparentna, ili prihvatljiva u smislu troškova, trebali biste je izbjegavati kako biste spriječili nepredviđene troškove ili drugu štetu.

2.9. Prevarne ili obmanjujuće prakse kojih korisnici trebaju biti svjesni

Tehnološki napredak i nove mogućnosti koje daju mobilne aplikacije, te beskontaktno platne kartice i narukvice donose i rizike u smislu mogućih prevarnih ili obmanjujućih postupaka. Važno je napomenuti da se legitimna i provjerena upotreba aplikacija kontinuirano ažurira najnovijim softverskim rješenjima kako bi se ponudio najviši nivo zaštite od krađe podataka ili prevare. Međutim, čak i uz ove zaštite, važno je biti svjestan mogućih prevara i odgovornosti korisnika prilikom korištenja određene aplikacije ili linka, te prilikom dijeljenja podataka. S tim u vezi, najčešći primjeri prevare su socijalni inženjering, odnosno kada korisnik svojim djelovanjem omogući krađu podataka ili prevaru. Neki primjeri su navedeni u nastavku o phishingu, vishingu/glasovnom phishingu i smishingu.

- **Phishing** uključuje različite tehnike socijalnog inženjeringa koje se koriste za krađu podataka od korisnika finansijskih usluga. Žrtva se često kontaktira putem popularnih društvenih mreža sa primamljivim ponudama ili linkovima. Ova vrsta prevare može se pojaviti u obliku atraktivnih ili primamljivih naslova, obećanja, naizgled vjerodostojnog sadržaja koji ima za cilj navesti korisnika da klikne i uspostavi vezu. Najčešće ovi pokušaji uključuju vishing i smishing.

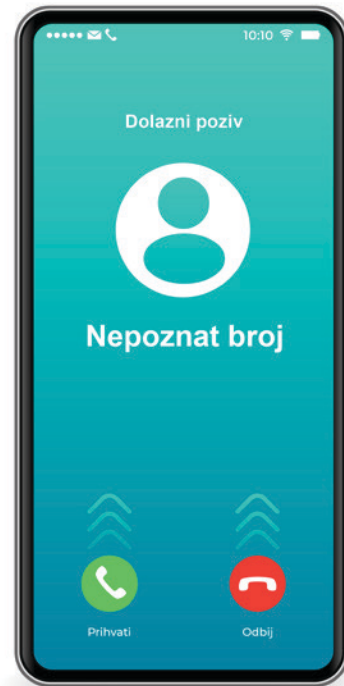




- **Vishing**, ili glasovni phishing, dešava se kada se žrtva kontaktira putem telefona uz lažno predstavljanje i od nje se traže podaci o platnim karticama, bankovnim računima itd.

Primjer vishinga

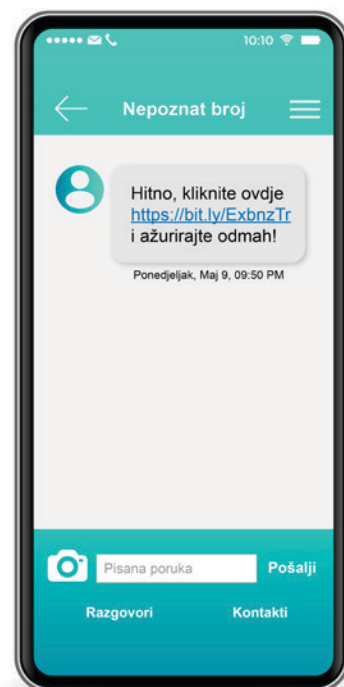
Žrtva koristi beskontaktnu platnu karticu za svakodnevne kupovine. Jednoga dana iznenada dobije poziv sa nepoznatog broja i osoba koja se predstavlja kao službenik banke hitno zahtijeva podatke o kartici za provjeru uplate od 100 KM na osnovu nagrade koju je žrtva osvojila u banci.



- **Smishing**, ili tekstualni phishing, dešava se kada se s nepoznatog broja pošalje SMS ili poruka iz aplikacije za časkanje sa primamljivim sadržajem koji poziva žrtvu da klikne na određeni link. Otvaranjem linka primalac često nevoljno instalira malware, odnosno štetnu aplikaciju koja može ukrasti njegove lične podatke s mobilnog uređaja.

Primjer smishinga

Osoba koja koristi aplikaciju za mobilno plaćanje iznenada dobije SMS sa nepoznatog broja da od sljedećeg dana više neće raditi aplikacija za plaćanje instalirana na njegovom mobilnom uređaju i da odmah instalira novu putem priloženog linka na SMS.



Osim ovih primjera, postoje i druge prevarne prakse koje imaju isti cilj da zloupotrijebe podatke korisnika kako bi dobili neovlašteni pristup i izvršili nezakonite transakcije. Još jedna česta praksa prevare je skraćeni URL, web adresa, koja često (iako ne uvijek) maskira zlonamjerni URL namijenjen omogućavanju prevare. Zato je važno biti na oprezu. Važno je znati da su skraćeni URL-ovi česti čak i kod legitimne upotrebe, na primjer, društvenih medija (iako je u takvim slučajevima moguće vidjeti i punu adresu). Ali u slučajevima maliciozne namjere, korisniku je teško vidjeti punu URL adresu (skriveni podaci), pa bi korištenje ovih adresa moglo navesti korisnika da posjeti lažne web stranice. Imajte na umu da uvijek posjećujete legitimne web stranice. Saznajte više o "sigurnim opcijama" web stranica.

Važno je biti oprezan i uvijek se pridržavati osnovnih sigurnosnih pravila:



- 1 Koristite antivirusni softver na svom pametnom telefonu
- 2 Redovno ažurirajte svoje aplikacije
- 3 Instalirajte samo aplikacije iz službene online trgovine
- 4 Zapamtite i ne dijelite svoje pristupne informacije (lozinke, PIN, itd.)
- 5 Razmislite o korištenju potvrde u 2 koraka (trenutno većina vodećih platformi i aplikacija nudi opciju verifikacije u 2 koraka)
- 6 Budite informirani o opcijama tokenizacije (koristeći token za digitalnu identifikaciju) ili osigurajte svoje transakcije verifikacijom u 2 koraka putem SMS-a
- 7 Ne klikajte na sadržaj iz neprovjerenih ili sumnjivih izvora
- 8 Nikada ne dijelite podatke o svojoj kartici
- 9 Pokrijte tastaturu kada unosite PIN u POS terminal
- 10 Redovno provjeravajte svoje bankovne izvode i odmah prijavite sve neuobičajene transakcije vašoj banci
- 11 Ako korištenje aplikacije ili drugog digitalnog načina plaćanja uključuje prihvatanje odredbi i uslova, pročitajte ih prije prihvatanja i tražite pojašnjenja gdje je potrebno
- 12 Nikada nemojte koristiti uređaje s hakovanim i/ili ilegalno otključanim (rooted, JailBroken, zakrpljenim) OS ili uređaje koji su korišteni za pristup ilegalnim web lokacijama, kao što su stranice za dijeljenje torenta, jer te stranice često sadrže zlonamjerni kod koji može zaraziti vaš uređaj i učiniti ga podložnim hakovanju i krađi ličnih podataka.

Ako korisnik plaćanja koristi aplikaciju za plaćanje na javnoj mreži ili nije siguran u sigurnosni nivo mreže za dijeljenje ličnih podataka, razmislite o korištenju enkripcije ili korištenja virtualne privatne mreže (VPN). Ako se koristi VPN, preporuka je da koristite provjereni VPN koji obično ima pretplatu.



2.10. Prava potrošača - korisnika, postupak prigovora i nadležne institucije za zaštitu prava potrošača

Korištenje opcija digitalnog plaćanja često je sigurno, ali sigurnost uključuje usvajanje odgovornih praksi i ponašanja korisnika. Nivo sigurnosti u procesu korištenja digitalnih plaćanja proporcionalan je stepenu odgovornosti korisnika usluga. Uprkos budnosti korisnika plaćanja, ponekad se dešavaju prevare i obmane. Ukoliko dođe do ovakvih slučajeva, korisnici plaćanja treba da budu upoznati sa okvirom zaštite prava potrošača i kako ga koristiti.

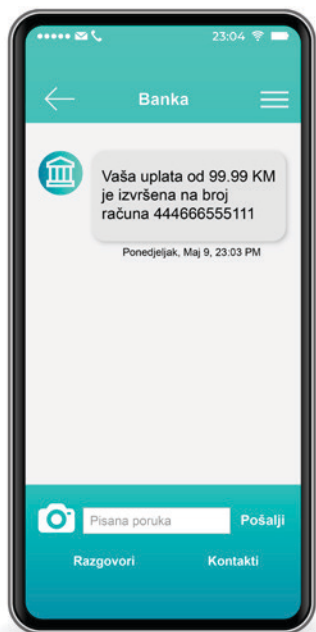
Ključni zakoni koji regulišu pravni okvir zaštite potrošača su Zakon o zaštiti prava korisnika finansijskih usluga FBiH, te Zakoni o bankama RS i FBiH. Ovi zakoni preciziraju prava i obaveze potrošača u svim fazama – od početne faze promocije i dogovaranja platnih usluga do završne faze potpisanog ugovora između pružaoca finansijskih usluga i korisnika plaćanja. Zakon takođe navodi prava i obaveze finansijskih institucija u pogledu nivoa potrebne transparentnosti i sigurnosti informacija. Zakoni propisuju odredbe koje ugovori o bankarskim uslugama moraju sadržavati uključujući precizne obaveze i prava stranaka, detalje usluge, cijenu i trajanje usluga, način obavještanja i izmjene ugovora, postupke za raskid ugovora, zaštitu prava i interesa korisnika itd.

Preporučljivo je pročitati opšte uslove prije korištenja bilo koje od opcija digitalnog plaćanja (ili bilo kojeg drugog finansijskog proizvoda ili usluge). Zakoni u BiH propisuju obaveze finansijskih institucija kada je u pitanju transparentnost usluga, što znači da svaka usluga treba biti pojašnjena kroz ugovor, ali i druge dokumente. Trebalo bi da pročitate ugovor i drugu dokumentaciju. Imate pravo da tražite pojašnjenje uslova i odredbi. Odredbe koje se odnose na obaveze ugovornih strana važne su za bolje razumijevanje koje obaveze pripadaju vama, a koje pružaocu usluge.



Prvo otkrivanje zloupotrebe

Prvi i najvažniji korak je da odmah prijavite svaku zloupotrebu ili grešku vašoj banci (npr. transakciju na vašem bankovnom izvodu koju niste odobrili, gubitak platne kartice ili narukvice, saznanje da ste instalirali aplikaciju koja sadrži zlonamjerni softver, itd.). Važno je pratiti stanje vašeg računa, provjeriti i pratiti lične podatke.



Banka će poduzeti jednostrane, neophodne korake da zaštiti vaš bankovni račun u zavisnosti od vrste izvještaja. U praksi, to može uključivati blokiranje vaše platne kartice ili narukvice, blokiranje plaćanja putem mobilnog telefona ili chata, dvostruku provjeru načina na koji je transakcija izvršena i da li je postojala autorizacija ili druga radnja koja se smatra potrebnom u datoj situaciji.



Šta ako je pristup usluzi privremeno obustavljen?

Da biste povratili pristup digitalnim bankarskim uslugama, novoj platnoj kartici ili narukvici, potrebno je svojoj banci podnijeti pismeni izvještaj/prigovor. Pismeni izvještaj treba da sadrži detalje transakcije (npr. datum, ime subjekta/lično ime, iznos transakcije, sumnju na zloupotrebu podataka, itd.), zatražiti povrat sredstava na vaš račun (ako je bilo naplata ili povlačenja s vašeg računa bez vašeg odobrenja) kao rezultat prijavljene zloupotrebe. Korisnik treba da vodi evidenciju komunikacije između banke.

U skladu sa zakonskim i podzakonskim aktima, banka će pregledati ugovor korisnika i provjeriti okolnosti prijave. Banka će obavijestiti korisnika o poduzetim koracima i izvijestiti o podnesenom izvještaju/prigovoru.



Odmah prijavite zloupotrebu ili sumnjivu transakciju banci, ili gubitak kartice ili narukvice.



Banka će poduzeti neophodne korake da zaštiti vaš bankovni račun.

2.11. Ombudsmani za bankarski sistem

Ukoliko korisnik nije zadovoljan odgovorom banke ili nije dobio nikakav odgovor u roku od 30 dana od pisanog prigovora, može se obratiti ombudsmanu za bankarski sistem u nadležnoj entitetskoj agenciji za bankarstvo. Važno je napomenuti da se prigovori ombudsmanu za bankarski sistem mogu podnijeti u roku od šest mjeseci od dana prijema odgovora pružaoca usluge ili od isteka roka od 30 dana koji je propisan za odgovor pružaoca usluga. Postupak je besplatan.



Kontakt podaci entitetskih ombudsmana za bankarski sistem:

Agencija za bankarstvo Federacije BiH

Ombudsman za bankarski sistem

Adresa: Zmaja od Bosne 47b,
71000 Sarajevo

E-mail: ombudsmen@fba.ba

Telefon: 033 569 787

Agencija za bankarstvo Republike Srpske

Ombudsman za bankarski sistem

Adresa: Vase Pelagića 11a,
78000 Banja Luka

E-mail: info@abrs.ba

Telefon: 051 224 079

Po prijemu prigovora, u zavisnosti od svakog pojedinačnog slučaja, ombudsman će analizirati da li je prigovor opravdan. Ombudsman će izvršiti uvid u postupanje banke i korisnika, analizirati dostavljenu dokumentaciju koja pokazuje vremenski okvir razgovora između strana i razmotriti opravdanost prigovora. U zavisnosti od dobijenih informacija, ombudsman odlučuje da li će otvoriti slučaj. Ako ombudsman odluči da ne otvori slučaj, tada će savjetovati korisnika da traži dalje postupanje od druge relevantne institucije. U zavisnosti od situacije, to može uključivati ponovnu komunikaciju sa pružaocem finansijskih usluga ili zaštitu prava putem sudskog postupka. Ako ombudsman otvori predmet, vodi postupak po prigovoru i daje preporuku banci. Odluka ombudsmana nije pravno obavezujuća.



Važno je da prigovor sadrži potrebne i precizne podatke o transakciji, a uz prigovor treba priložiti odgovarajuću dokumentaciju.



Prigovor mora sadržavati:



- 1 Ime i prezime korisnika
- 2 Poštansku adresu korisnika i kontakt telefon/e-mail
- 3 Ime i prezime, adresu i kontakt telefon/e-mail punomoćnika korisnika (u slučaju da se prigovor šalje preko punomoćnika)
- 4 Poslovni naziv i adresu banke
- 5 Detaljne informacije o sporu između stranaka, kada i gdje se to dogodilo
- 6 Svi primjenjivi prilozi (npr. kopija prethodnog prigovora poslanog banci, kopija odgovora banke, kopija ugovora o bankarskim uslugama, drugi dokumenti povezani sa sporom kao što je punomoć, itd.)
- 7 Datum i mjesto vašeg prigovora
- 8 Potpis (u slučaju slanja pisma prigovora)

Preporuke/mišljenja ombudsmana nisu obavezujuće (za razliku od sudskih odluka), ali se mogu koristiti kao argumenti i bitni su u daljim postupcima (bilo kod finansijske institucije bilo suda), posebno imajući u vidu da ombudsman za bankarstvo djeluje u okviru Agencije za bankarstvo kao regulator komercijalnog finansijskog tržišta.

2.12. Posredovanje kao mogućnost vansudskog poravnanja

Alternativno, ako se strane slažu, preporuka može uključivati pokretanje postupka posredovanja kod ombudsmana za bankarski sistem kako bi se tražilo rješenje. U cilju rješavanja pitanja i zaštite prava, stranke se mogu dogovoriti da pokrenu postupak posredovanja kod ombudsmana za bankarski sistem i da na taj način traže rješenje.

Posredovanje je jedna od mogućnosti vansudskog poravnanja. Prednost postupka posredovanja je u tome što je fleksibilniji, jednostavniji i jeftiniji od sudskog postupka. Važno je istaći da je za pokretanje postupka neophodna saglasnost obje strane i da se postupak ne može pokrenuti jednostrano. Tokom posredovanja medijator (ombudsman) ne može nametati rješenja, ali može olakšati komunikaciju i pružiti stručne savjete kako bi pomogao strankama da nađu rješenje.

- ▶ Posredovanje je dobrovoljni postupak koji nije pravno obavezujući, ali je fleksibilniji i jeftiniji od sudskog postupka
- ▶ Stranke zajednički podnose zahtjev za pokretanje postupka posredovanja. Nije moguće podnijeti zahtjev jednostrano
- ▶ Zahtjev se podnosi u pisanoj formi
- ▶ Posrednik ne nameće rješenja, ali ona mogu pomoći u olakšavanju komunikacije i savjetima
- ▶ Sama procedura posredovanja je besplatna

Ukoliko ombudsman nije nadležan za dati prigovor, može savjetovati korisnika da traži dalje postupanje kod drugih relevantnih institucija i koje korake treba da poduzme.



S obzirom na to da se digitalna plaćanja često vrše za kupovinu robe i usluga, sporovi i prigovori se ponekad ne odnose na pružaoca digitalnih usluga, već na trgovca koji prodaje robu ili usluge. U takvim slučajevima primjenjuju se opšta pravila zaštite potrošača. U Bosni i Hercegovini kupovina, online kupovina ili kupovina na daljinu regulirana je zakonima o zaštiti potrošača i u nadležnosti je ombudsmana za zaštitu potrošača BiH. Više o instituciji ombudsmana za zaštitu potrošača u BiH možete saznati na www.ozp.gov.ba. Žalbe se mogu podnijeti direktno ili putem službene web stranice.



Zaštita prava se može ostvariti i putem suda. Pravosudni sistem u BiH, u zavisnosti od prirode zahtjeva ili povrede prava, pruža zaštitu u različitim postupcima. Korisno je, u slučaju traženja zaštite prava preko suda, konsultovati se i tražiti stručnu pravnu pomoć.



Upitnik za čitaoce da procijene svoje znanje

Imajte na umu da je na svako pitanje moguć samo jedan tačan odgovor

1

Koja je glavna karakteristika bezgotovinskog plaćanja?

- a) Transakcija se odvija bez fizičkog transfera novca
- b) Transakcija se odvija kreditnom karticom
- c) Transakcija se odvija samo za kupovinu putem interneta

2

Stvari koje ne možete učiniti s aplikacijom za mobilno bankarstvo?

- a) Provjeriti stanje na računu
- b) Napraviti nalog za plaćanje
- c) Potpisati ugovor

3

Beskontaktne platne kartice funkcionišu na osnovu koje tehnologije?

- a) NFC
- b) DFC
- c) FNC

4

Radi vaše sigurnosti, izuzetno je važno da:

- a) Zapamtite svoj PIN broj i podijelite ga sa nekim bliskim prijateljima (za pomoć u slučaju da se ne možete sjetiti)
- b) Zaštite sve svoje podatke, kao i svaki pristup aplikaciji, od zloupotrebe korištenjem PIN-a ili lozinke i biometrije
- c) Prilikom odabira šifre ili PIN-a, koristite jednostavne kombinacije brojeva kako biste aplikaciju učinili lakšom za korištenje

5

Koji su najčešći primjeri prevare?

- a) Vishing
- b) Pozivanje
- c) Ćaskanje

6

Ako primijetite neuobičajenu transakciju, zloupotrebu ili grešku aplikacije za mobilno plaćanje, prvo što trebate učiniti je da:

- a) Redovno ažurirate svoju aplikaciju za mobilno plaćanje
- b) Odmah prijavite svaku zloupotrebu ili grešku vašoj banci dajući potrebne informacije
- c) Kontaktirate primaoca transakcije i zatražite pojašnjenje

7

Koji zakoni regulišu zaštitu potrošača finansijskih usluga u entitetima?

- a) Zakon o finansijskim institucijama u Federaciji BiH i Republici Srpskoj
- b) Zakon o zaštiti korisnika finansijskih usluga Federacije BiH i Zakon o bankama Republike Srpske
- c) Zakon o zaštiti potrošača finansijskih sredstava u Federaciji BiH i Republici Srpskoj

8

Koja je uloga ombudsmana za bankarski sistem?

- a) Štiti ljudska i radna prava zaposlenih u finansijskim institucijama
- b) Štiti prava i interese banaka
- c) Štiti prava i interese korisnika finansijskih usluga i proizvoda

9

Korisnik finansijskih usluga može uputiti pismeni prigovor ombudsmanu za bankarski sistem u nadležnoj entitetskoj agenciji za bankarstvo.

- a) Ukoliko korisnik nije zadovoljan odgovorom pružaoca usluge ili nije dobio nikakav odgovor u roku od 30 dana od pisanog izvještaja
- b) Ako korisnik nema povjerenja u pružaoca usluga i uopće ne želi komunikaciju
- c) Ako je korisnik za plaćanje koristio neregulisanu uslugu

10

Prigovor ombudsmanu za bankarski sistem može se podnijeti u roku:

- a) dvanaest mjeseci od datuma prijema odgovora pružaoca usluga
- b) devet mjeseci od dana prijema odgovora pružaoca usluga
- c) šest mjeseci od dana prijema odgovora pružaoca usluga

11

Koju opciju nudi ombudsman za bankarski sistem kao vansudsko rešenje spora?

- a) Posredovanje
- b) Pomirenje
- c) Zastupanje pred sudom

12

Zakoni (koji propisuju norme o zaštiti potrošača korisnika finansijskih usluga/proizvoda) u BiH propisuju obaveze finansijskih institucija kada je u pitanju:

- a) Raspon cijena usluga digitalnog plaćanja
- b) Transparentnost usluge i prava i obaveze potrošača u svim fazama
- c) Korištenje verifikacije u 2 koraka na aplikacijama za mobilno plaćanje

Spisak tačnih odgovora iz upitnika

Pitanje	Tačan odgovor	Pitanje	Tačan odgovor
1	A	7	B
2	C	8	C
3	A	9	A
4	B	10	C
5	A	11	A
6	B	12	B

Rječnik osnovnih pojmova korištenih u Vodiču

ATM

Bankomat (ATM) je elektronska banka koja omogućava klijentima da završe osnovne transakcije bez pomoći predstavnika filijale ili blagajnika. Svako ko ima kreditnu ili debitnu karticu može pristupiti gotovini na većini bankomata.

Bankovni račun

Bankovni račun je finansijska usluga/proizvod. To je račun koji vodi banka i koristi se za plaćanja i depozite. Svaka finansijska institucija (banka) postavlja uslove za svaku vrstu računa koji nudi.

Beskontaktno plaćanje

Beskontaktno plaćanje omogućavaju vlasniku takve kartice da vrši plaćanja na POS terminalima dodiranjem platne kartice na beskontaktni POS uređaj. Narukvice za beskontaktno plaćanje temelje se na istom principu kao i beskontaktno plaćanje platne kartice jer sadrže mini kartice koje je potrebno prisloniti na beskontaktno POS terminale za plaćanje.

Debitna kartica

Debitna kartica je povezana sa tekućim bankovnim računom. Sredstva koja su dostupna na računu troše se debitnom karticom.

Digitalne finansijske usluge

Finansijske usluge podržane modernim tehnologijama i koje se nude putem mobilnih telefona, POS uređaja i interneta. Usluge koje se nude digitalno mogu dramatično smanjiti troškove za kupce i pružaoce usluga.

Prava zaštite potrošača finansijskih usluga

Prava zaštite potrošača finansijskih usluga propisana su nizom zakona i propisa koje donose regulatorne institucije i predstavljaju pravni okvir za zaštitu korisnika finansijskih proizvoda i usluga.

Finansijska institucija/pružalac finansijskih usluga

Finansijska institucija je društvo koje se bavi pružanjem finansijskih usluga i proizvoda i finansijskim i monetarnim transakcijama kao što su depoziti, krediti, plaćanja, investicije i mijenjanje valuta. U Bosni i Hercegovini najčešće finansijske institucije na tržištu su banke, mikrokreditne organizacije i lizing kompanije.

Prevara

Prevara je postupak obmane u kojoj je jednu osobu finansijski prevarila druga osoba. Postoji mnogo različitih vrsta prevara u finansijama ili bankarstvu. Neke od najčešćih vrsta prevara su prevara s debitnim i kreditnim karticama, krađa identiteta, prevara u digitalnom plaćanju, prevara u sefovima itd.

Malware

Malware (skraćeno od "zlonamjerni softver" (eng. malicious software)) je datoteka ili kod (isporučen preko mreže), osmišljen tako da poremeti, ošteti, ukrade ili dobije neovlašteni pristup računarskom sistemu.

Posredovanje

Posredovanje je jedno od mogućnosti vanskodnog rješavanja spora. Prednost postupka posredovanja je što je fleksibilniji, jednostavniji i jeftiniji od sudskog postupka.

Mobilna aplikacija

Mobilna aplikacija ili app je softverska aplikacija ili računarski program dizajniran za rad na mobilnom uređaju kao što je pametni telefon, tablet ili pametni sat.

Mobilno bankarstvo

Mobilno bankarstvo koristi mobilne telefone kao kanal za pružanje finansijskih usluga. Mobilno bankarstvo podržava platne transakcije uključujući transfere novca, tekuće račune, a u nekim slučajevima i otplatu kredita, lično planiranje itd.

Mobilno plaćanje

Mobilno plaćanje je finansijska transakcija izvršena putem mobilnog uređaja ili drugog prenosnog elektronskog uređaja. To je finansijski proizvod ili usluga. Mobilno plaćanje je finansijska usluga i proizvod i može se koristiti i za slanje novca drugima.

NFC (komunikacija bliskog polja)

Komunikacija bliskog polja (NFC) je skup komunikacijskih protokola koji omogućava komunikaciju između dva elektronska uređaja na određenoj udaljenosti (od 4 cm ili manje).

Ombudsmeni za bankarski sistem u Bosni i Hercegovini

Ombudsman za bankarski sistem je institucija osnovana na entitetskom nivou radi promocije i zaštite prava i interesa građana kao korisnika finansijskih usluga. Postoje različiti mehanizmi za zaštitu prava, kao što su postupak po prigovoru ili posredovanje.

Odobrenje plaćanja

Odobrenje plaćanja je proces koji verifikacijom čini plaćanje sigurnijim. Identifikacija korisnika prilikom otvaranja aplikacije za plaćanje i odobrenje plaćanja provode se putem PIN-a ili lozinke koji je poznat samo korisniku, ili putem biometrijskih podataka korisnika (otisak prsta i/ili skeniranje mrežnice).

Lozinka

Lozinka je numerički niz koji se koristi za potvrđivanje identiteta korisnika na računaru ili drugom elektronskom uređaju.

Phishing

Phishing je prevara kao praksa sajber napada koji se često koristi za krađu korisničkih podataka, uključujući podatke za prijavu i brojeve kreditnih kartica. Najčešća praksa napada je kada je primalac prevaren da klikne na zlonamjerni link.

PIN

Lični identifikacioni broj (PIN) je numerički kod koji se koristi kao mehanizam identifikacije, uglavnom u elektronskim finansijskim transakcijama. Lični identifikacioni brojevi se obično izdaju u vezi sa platnim karticama, mobilnim bankarstvom, te raznim oblicima digitalnog plaćanja i mogu biti potrebni za dovršetak transakcije.

Uređaj na prodajnom mjestu (POS)

Mali, prenosivi uređaj koji olakšava elektronsku finansijsku transakciju. POS uređaji u određenim slučajevima mogu poslužiti i kao mjesto bankarskog poslovanja. Ovaj uređaj se koristi u trgovanju i kupovini prilikom bezgotovinskog plaćanja raznih roba i usluga. Budući da su jeftini i lako prenosivi, igraju važnu ulogu u premošćavanju lokacijskog jaza i omogućavanju pristupa finansijskim uslugama u ruralnim područjima i područjima sa nerazvijenom infrastrukturom.

QR code

Brzi odgovor ili QR kod je dvodimenzionalna verzija barkoda, koja se obično sastoji od crnih i bijelih uzoraka piksela. QR kod sadrži određene informacije (različitih tipova) koje softver može lako pročitati. QR kod olakšava provođenje procesa plaćanja itd.

SMS (usluga kratkih poruka)

Usluga kratkih poruka ili SMS je tehnologija za slanje kratkih tekstualnih poruka između mobilnih telefona. SMS se često koristi za verifikaciju (korištenje usluga, plaćanja, itd.).

Vishing

Vishing je praksa prevare, kombinacija 'glasa' i 'phishinga'. To je telefonska prevara ili glasovna poruka dizajnirana da navede korisnika da podijeli lične podatke.

VPN (Virtual Private Network)

Virtualna privatna mreža ili VPN je šifrovana veza između uređaja i internet mreže. Glavna svrha VPN-a je uspostavljanje zaštićene mrežne veze prilikom korištenja javnih mreža i pomaže u zaštiti prenosa podataka..

Prijedlog korisnih linkova

Korisni linkovi institucija

Centralna banka Bosne i Hercegovine: www.cbbh.ba

Centralna banka Bosne i Hercegovine - web stranica o finansijskoj edukaciji: fined.cbbh.ba

Agencija za bankarstvo Federacije BiH / Ombudsmeni za bankarski sistem:

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

www.fba.ba/objection-form/1760

E-mail: ombudsman@fba.ba

Agencija za bankarstvo Republike Srpske / Ombudsmeni za bankarski sistem:

www.abrs.ba; www.abrs.ba/lat/ombudsman/c90;

E-mail: info@abrs.ba

Pratite nas:



www.cbbh.ba

Twitter: [@CBBiH](https://twitter.com/CBBiH)

YouTube kanal: [Centralna banka Bosne i Hercegovine](https://www.youtube.com/CentralnaBankaBiH)

Facebook: www.facebook.com/CentralnaBankaBiH

LinkedIn: www.linkedin.com/company/cbbih

Centralna banka Bosne i Hercegovine

Služba za odnose sa javnošću

pr@cbbh.ba

contact@cbbh.ba

+387 (33) 278 123

+387 (33) 201 517



Svjetska banka

E-mail: bih@worldbank.org

Telefon: +387 (33) 251 500

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

Facebook: [@WorldBankBiH](https://www.facebook.com/WorldBankBiH)





Centralna banka Централна банка
BOSNE I HERCEGOVINE БОСНЕ И ХЕРЦЕГОВИНЕ



WORLD BANK GROUP
Finance, Competitiveness & Innovation