Sigurnost HPB mobilnog bankarstva

Kao korisnik interneta i mobilnog bankarstva izloženi ste sigurnosnim rizicima kibernetičkih napada i pokušajima prijevara trećih strana. Molimo Vas koristite ove smjernice kao preporuke za povećanje razine vaše sigurnosti pri korištenju usluge HPB mobilnog bankarstva i mtokena (mHPB).

Što možete učiniti sami u svrhu zaštite svojih podataka i mobilnog uređaja

- **Zaštita aktivacijskog koda** nakon ugovaranja usluge ili ponovne aktivacije mHPB od Banke ćete dobiti aktivacijski kod koji se sastoji se od dva dijela i koji obvezno zaštitite i čuvajte na sigurnom mjestu do aktivacije usluge. Jedan dio aktivacijskog koda korisnik dobiva u Banci, a drugi se iz sigurnosnih razloga korisniku dostavlja odvojenim kanalom
- **Brinite o sigurnosti lozinki i PIN-ova** - ne otkrivajte svoj PIN nikome, ne pohranjujete ga na mobilni uređaj ili računalo, nemojte ga zapisivati i držati uz mobilni uređaj ili računalo, token ili m-token te obvezno sakrijete postupak unosa PIN-a od pogleda drugih osoba. Pri određivanju PIN-a za mHPB odredite PIN koji je teško pogoditi. Ukoliko sumnjate da je druga osoba vidjela Vaš PIN, odmah ga promijenite putem mHPB-a
- **Preuzimajte i redovno ažurirajte mHPB aplikaciju isključivo iz službenih trgovina,** Google Play, Apple App Store ili Huawei AppGalery, ovisno o proizvođaču vašeg mobilnog uređaja

Važno! Nikada ne preuzimajte i ne instalirajte mHPB aplikaciju iz nepoznatih i neprovjerenih izvora.

- Redovito provjeravajte jesu li dostupne **nove verzije operativnog sustava i redovito ažurirajte operativni sustav Vašeg mobilnog uređaja**
- **Podesite zaključavanje ekrana Vašeg mobilnog uređaja** i otključavajte ga putem PIN-a ili biometrije samo kad ga koristite
- **Nikada ne ostavljajte mobilni uređaj s otključanim ekranom ili bez nadzora,** posebno to nemojte učiniti ako još niste odjavljeni iz mHPB aplikacije
- **Budite oprezni pri korištenju mHPB aplikacije putem interneta koji je dostupan na javnim mjestima** (poput kafića, hotela i dr.) i isključite Bluetooth vezu dok nemate potrebu dijeljenja svojih informacija s drugima
- **Ne pokazujte ekran** svog mobilnog uređaja drugim osobama dok koristite mHPB aplikaciju
- Instalirajte i redovito ažurirajte **programe za zaštitu od zlođudnog koda** renomiranih proizvođača isključivo iz službene trgovine na Vašem mobilnom uređaju kojim se koristite za pristup mHPB aplikaciji

- Obratite pozornost i zaštitite se od **prijevarnih elektroničkih poruka:**
  - ne otvarajte i ne postupajte po prijevarnim elektroničkim porukama koje od vas traže da se prijavite u mobilno bankarstvo ili promijenite lozinku ili PIN, to su moguće prijevarne poruke
  - ne otvarajte neželjene poruke za koje niste sigurni tko je pošiljatelj ili su označene kao „spam“, posebno ne otvarajte one koje uz navedeno dodatno sadrže linkove ili privitke

Važno! Banka Vam nikada neće poslati neočekivanu e-poruku s poveznicom (linkom) na svoje stranice za prijavu u HPB mobilno bankarstvo**.** Ako dobijete takvu e-poruku, ona sigurno nije od Banke i izbrišite ju.

- **Izbjegavajte i/ili nemojte činiti slijedeće rizične radnje:**
  - ne otvarajte dokumente i aplikacije koje ste pribavili putem interneta iz sumnjivih i nepouzdanih izvora ili koje ne možete provjeriti programima za zaštitu od zlćudnog koda renomiranih proizvođača
  - ne dozvolite obradu svojih osobnih i kontakt podataka te podataka o svojim računima i karticama sumnjivim i nepouzdanim trećim stranama, osobama ili internetskim servisima
  - ne pokrećite i ne instalirajte sumnjive aplikacije ili dodatke za pristup mHPB aplikaciji – Banka od Vas takvo što neće tražiti
  - ne šaljite personalizirane sigurnosne podatke koji se inače koriste za potrebe ili unutar mHPB aplikacije u svrhu prijave ili autorizacije (npr. PIN, OTP), bilo kojim trećim osobama, uključujući zaposlenike Banke

Važno! Zaposlenici Banke Vas nikada neće tražiti odavanje povjerljivih podataka kao što su lozinke, PIN-ovi, autentifikacijski i autorizacijski kodovi generirani tokenom ili m-tokenom ili druge personalizirane sigurnosne podatke. Iznimku od tog pravila predstavlja jedino slučaj tajne riječi koju Banka koristi u formalnom postupku otključavanja tokena. Personalizirani sigurnosni podaci služe isključivo vama i važno je da ih nikada ne odajete bilo kojim trećim osobama, slučajno ili namjerno, bilo kojim načinom komunikacije (usmeno, telefonom, porukama, elektroničkom poštom, dijeljenjem ekrana mobitela ili računala, slanjem slika ekrana mobitela ili računala ili bilo kojim drugim načinom).

- **Promjena mobilnog uređaja** Na novom uređaju preuzmite mHPB aplikaciju iz ovlaštene trgovine i aktivirajte koristeći aktivacijske kodove koje vam je izdala Banka. Za mobilni uređaj koji više ne koristite preporučamo povrat na tvorničke postavke kako biste izbrisali sve svoje podatke
- **Informirajte se o sigurnosti usluge Banke i obavezno čitajte poruke Banke** u Vašem pretincu unutar mHPB aplikacije i na javnim web-stranicama Banke (www.hpb.hr)
- **Provjerite podatke na nalogu prije potvrde plaćanja,** posebno iznos plaćanja, IBAN ili broj računa primatelja i poziv na broj
- **Redovito provjeravajte stanje i promete po svojim računima**
- **Odjava** – odmah po završetku korištenja HPB mobilnog bankarstva ili mTokena odjavite se iz mHPB aplikacije i zaključajte ekran Vašeg mobilnog uređaja

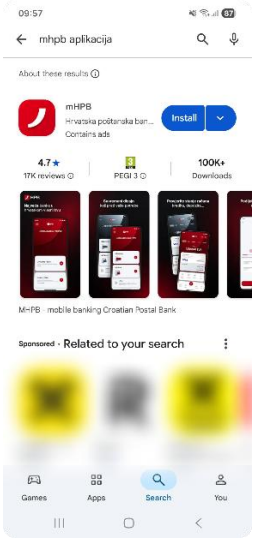
- **Dodatno se informirajte** o mogućim prijevarama i savjetima putem web stranica Hrvatske udruge banaka: https://www.hub.hr i stranica Nacionalnog CERT-a: https://www.cert.hr

HPB mobilno bankarstvo

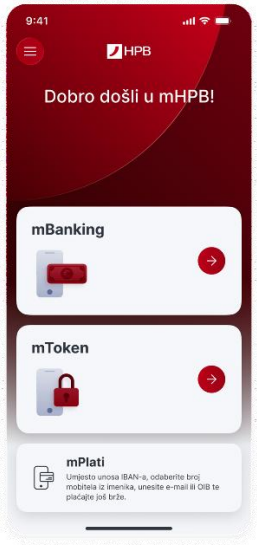
- **HPB mobilnom bankarstvu ili m-Tokenu** pristupajte izravno s vašeg mobilnog uređaja na kojem ste instalirali mHPB aplikaciju koju ste preuzeli iz službenih trgovina

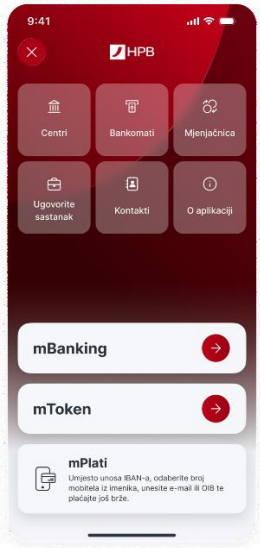
Download on the App Store | GET IT ON Google Play | EXPLORE IT ON AppGallery

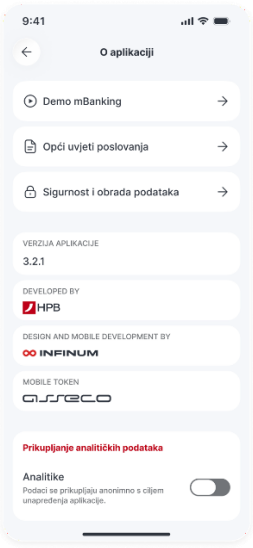
  - primjer ako za preuzimanje mHPB aplikacije koristite Play Store:



- **Aktivacija mHPB-a** provodi se korištenjem **aktivacijskog koda** – personalizirani sigurnosni podatak koji Banka dodjeljuje Korisniku u svrhu aktivacije mobilne usluge
- **Za prijavu na mHPB** u svrhu autentifikacije korisnik unosi PIN ili primjenjuje biometrijsku metodu, ovisno o tome što je odabrao kod aktivacije mobilne usluge mHPB na svom mobilnom uređaju
  - primjer prijavne stranice mHPB aplikacije, dostupne informacije i informacije o aplikaciji:







- Korisnik može odabrati prijavu u mHPB **metodom biometrijske autentifikacije**, otisak prsta/Touch ID ili prepoznavanje lica/Face ID, ovisno o proizvođaču i/ili dostupnosti navedenih metoda unutar operativnog sustava mobilnog uređaja korisnika

Važno! Prestanite s radom na mobilnom uređaju ako na prijavnoj stranici mHPB aplikacije primijetite bilo koji od slijedećih problema:

- prijavna stranica za mHPB izgleda neuobičajeno, primjerice postoje dva polja za unos PIN-a, stranica sadrži gramatički neispravan tekst ili se umjesto dijakritičkih znakova (č, ć, đ, š i ž) prikazuju čudni simboli
- ako Vas mHPB aplikacija u svrhu prijave traži neki drugi ili dodatni podatak osim PIN-a ili biometrije, poput autentifikacijskih kodova koji se koriste u svrhu autorizaciju transakcija (APPLI2/MAC ili APPLI3/MDS) ili da ponovite unos PIN-a nakon što ste sigurni da ste ga uspješno unijeli i potvrdili prvi puta
- ako Vas neka osoba koja se može predstavljati i kao zaposlenik Banke traži dostavu podataka za prijavu u HPB mobilno bankarstvo putem nekog drugog kanala (elektroničke poruke, SMS-a i sl.) – ti podaci se koriste isključivo unutar aplikacije HPB internetskog bankarstva.

Ukoliko uočite nepravilnosti molimo vas da ih **prijavite na** hpb@hpb.hr **ili telefonskim pozivom. Kontakt za pozive unutar HR: 0800 472 472 i kontakt za pozive iz inozemstva: +00 385 1 489 0365.**

- **Za prijavu u HPB mobilno bankarstvo ili mToken** uvijek je potrebno unijeti samo PIN ili koristiti odabranu metodu biometrijske autentifikacije - ova radnja predstavlja snažnu ili pouzdanu autentifikaciju korisnika koja je detaljnije opisana kasnije u tekstu
- **Autorizacija naloga za plaćanje i spremanje primatelja na Listu provjerenih primatelja** - nakon uspješne prijave i samo unutar mHPB za radnje autorizacije naloga ili za spremanje primatelja na Listu provjerenih primatelja korisnik mora provesti autentifikaciju unosom PIN-a ili primjenom biometrijske metode. Temeljem navedene autentifikacije mHPB aplikacija generira autorizacijski kod APPLI2/MAC ili APPLI3/MDS, a za dodavanje na Listu provjerenih primatelja APPLI3/MDS. Za radnje više razine rizika koje provodite putem mobilnog bankarstva, Banka primjenjuje snažnu ili pouzdana autentifikaciju klijenta, kako je detaljnije opisana kasnije u tekstu na primjeru APPLI3/MDS postupka. Dodatno, u istom postupku i nakon uspješnog zadavanja transakcije možete odabrati želite li primatelja dodati na listu Provjerenih primatelja. Listu provjerenih primatelja stvarate sami i ona jednako vrijedi na HPB internetskom i mobilnom bankarstvu.

Zaštitne mjere Banke

- **Autentičnost komunikacijskih sudionika mHPB aplikacije i servisa Banke jamči se primjenom digitalnih certifikata** – primjenjuje se obostrana provjera
- **Zaštita podataka u prijenosu** - pri prijenosu podataka koristi se TLS protokol. Svi podaci koje korisnik putem mHPB aplikacije izmjenjuje s poslužiteljem HPB-a u svakom su trenutku šifrirani (kriptirani) uporabom tog protokola
- **Zaključavanje mobilnog bankarstva** - nakon određenog broja uzastopnog unosa pogrešnog PIN-a, aplikacija mHPB se zaključava i prijava u mHPB će Vam biti onemogućena
- **Automatska odjava** - ako ste prijavljeni u mHPB, ali ste određeno vrijeme neaktivni, biti ćete automatski odjavljeni
- **Objave o sigurnosnim prijetnjama** - kako bi Vas upozorila na pojavu novih prijetnji i postupaka koje implementira da bi Vas zaštitila, Banka objavljuje obavijesti na svojim web stranicama i dostavlja ih porukom u Vaš pretinac unutar HPB mobilnog bankarstva
- **Snažna ili pouzdana autentifikacija korisnika u svrhu prijave** - kod pristupa HPB mobilnom bankarstvu Banka primjenjuje **snažnu** dvofaktorsku autentifikacija korisnika APPLI1/OTP. Pri tom je jedan faktor autentifikacije nešto što korisnik ima: mToken, a drugi faktor nešto što korisnik zna ili je: PIN ili biometrija.
- **Autorizacija naloga za plaćanje** - Banka će za potvrdu podataka za običnu autorizaciju, kada zadajete nalog za plaćanje primatelju koji se nalazi na Listi provjerenih primatelja, od Vas tražiti provjeru podataka na nalogu te unos PIN-a ili korištenje biometrijske autentifikacije i generirati i primijeniti APPLI2/MAC kod
- **Snažna ili pouzdana autentifikacija korisnika u svrhu autorizacije transakcije ili dodavanja na Listu provjerenih primatelja** - kako bi smanjila mogućnost zloupotrebe u slučaju kompromitacije na strani klijenta, kada zadajete nalog za određeno plaćanje prema primatelju koji nije na Vašoj Listi provjerenih primatelja ili dodajete primatelja na Vašu Listu, Banka primjenjuje **snažnu** dvofaktorsku autentifikaciju korisnika i **dinamičko povezivanje** te će Vas tražiti provjeru podataka na nalogu ili podataka o primatelju kojeg dodajete na listu te unos PIN-a ili korištenje biometrijske autentifikacije i generirati i primijeniti APPLI3/MDS kod. Navedena autorizacija kod pokretanja postupka generiranja koda za autorizaciju, osim dvofaktorske autentifikacije, u svrhu **dodatne provjere s Vaše strane**, traži provjeru i potvrdu polja koja su dinamički povezana s konkretnom transakcijom koju autorizirate. Kod primjera naloga za plaćanje, a prije potvrde s Vaše strane, obvezno provjerite prvo važno polje: IBAN ili broja računa primatelja i drugo važno polje: iznos transakcije.

Zaštitne mjere kada klijent Banke koristi usluge drugih licenciranih pružatelja platnih usluga

Prema Zakonu o platnom prometu, klijenti Banke koji su korisnici usluge HPB internetskog ili mobilnog bankarstva za sve svoje transakcijske račune koje Banka vodi, mogu koristiti usluge iniciranja plaćanja i usluge informiranja o računu koje pružaju licencirani pružatelj navedenih usluga. Zaštitne mjere Banke navedene u ovom dokumentu, a koje se odnose na postupke autentifikacije i autorizacije (APPLI1/OTP, APPLI2/MAC i APPLI3/MDS) koje klijent provodi unutar HPB mobilnog bankarstva, u jednakoj mjeri primjenjuju se i za postupke autentifikacije i autorizacije koje provodite posredstvom licenciranih pružatelja usluga, a Banka ih provodi automatskim preusmjeravanjem na odgovarajuće stranice Banke ili iniciranjem push poruka na mobilnu aplikaciju Banke (mHPB).

Hrvatska poštanska banka, dioničko društvo