# Sigurnost HPB internetskog bankarstva

Kao korisnik interneta i internetskog 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 internetskog bankarstva.

## Što možete učiniti sami u svrhu zaštite svojih podataka i osobnog računala

- **Brinite o sigurnosti lozinki i PIN-ova** - ne otkrivajte svoj PIN nikome, ne pohranjujete ga na računalo, nemojte ga zapisivati i držati uz računalo, token ili mToken te obvezno sakrijete postupak unosa PIN-a od pogleda drugih osoba.
- Obratite pozornost i zaštitite se od **prijevarnih elektroničkih poruka:**
  - ne otvarajte i ne postupajte po elektroničkim porukama koje od vas traže da se prijavite u HPB internetsko 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 i linkove ili privitke.

**Važno!** Banka Vam nikada neće poslati neočekivanu e-poruku s poveznicom (linkom) na svoje stranice za prijavu u HPB internetsko 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 izvršne programe koje ste pribavili putem interneta iz sumnjivih i nepouzdanih izvora ili koje ne možete provjeriti programima za zaštitu od zloćudnog 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 programe ili dodatke za pristup HPB internetskom bankarstvu - Banka od Vas takvo što neće tražiti
  - ne šaljite personalizirane sigurnosne podatke koji se inače koriste za potrebe ili unutar HPB internetskog bankarstva 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 mTokenom 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).

- **Informirajte se o sigurnosti usluge Banke i obavezno čitajte poruke Banke** u Vašem pretincu unutar HPB internetskog bankarstva i na javnim web-stranicama Banke (www.hpb.hr).
- **Provjerite podatke na nalogu prije potvrde plaćanja**, posebno iznos plaćanja, IBAN ili broj računa primatelja te poziv na broj.
- **Redovito provjeravajte stanje i promete po svojim računima.**
- Instalirajte i redovito ažurirajte **programe za zaštitu od zlćudnog koda** renomiranih proizvođača na vašem osobnom računalu kojim se koristite za pristup HPB internetskom bankarstvu.
- **Odjava –** odmah po završetku korištenja HPB internetskog bankarstva odjavite se klikom na gumb „Odjava".
- **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

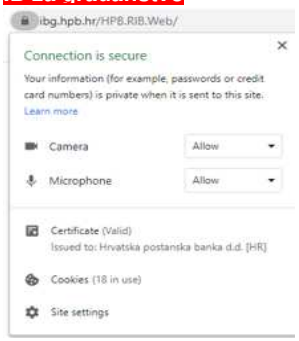
## HPB internetsko bankarstvo

- **HPB Internetskom bankarstvu** pristupajte izravno putem službene web-stranice Banke www.hpb.hr i u gornjem desnom kutu odaberite eBankarstvo te potom odaberite opciju prijave u IB

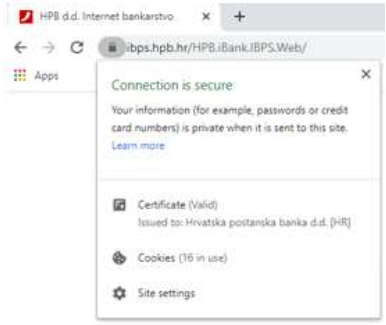

**Važno!** U HPB internetsko bankarstvo nikada se nemojte prijavljivati putem linkova iz elektroničkih poruka ili putem poveznica s drugih internetskih stranica.

- **Prije prijave** (unosa serijskog broja tokena i jednokratne lozinke), **provjerite nalazite li se na stranici Banke** na način da u adresnom polju (ispred ili iza URL adrese), kliknete na lokot i provjerite valjanost certifikata web stranice i sigurnost konekcije
  - primjer provjere ako koristite Google Chrome pretraživač:

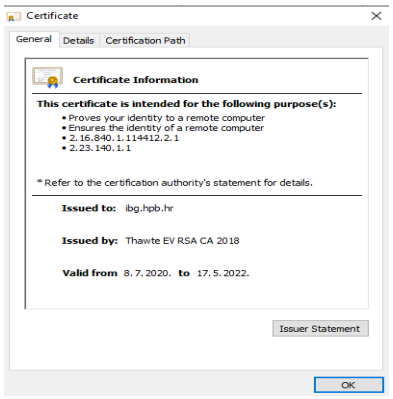
**IB za građanstvo**

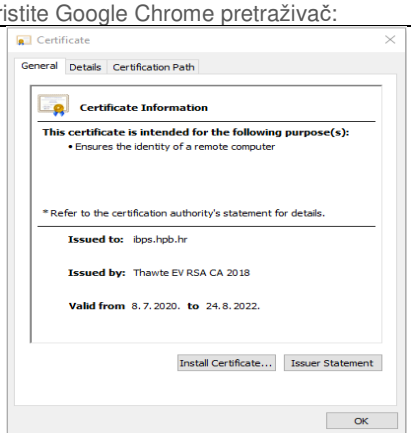



**IB za poslovne subjekte**



- primjer provjere detalja certifikata ako koristite Google Chrome pretraživač:




**Važno!** Prestanite s radom na računalu ako na prijavnoj stranici za HPB internetsko bankarstvo primijetite bilo koji od slijedećih problema:

- valjanost certifikata nije potvrđena („Invalid“) ili certifikat nije izdan za internetsku domenu **ibg.hpb.hr**
- prijavna stranica izgleda neuobičajeno, primjerice postoje dva polja za unos jednokratne lozinke, stranica sadrži gramatički neispravan tekst ili se umjesto dijakritičkih znakova (č, ć, đ, š i ž) prikazuju čudni simboli
- ako Vas stranica za prijavu traži neki drugi ili dodatni podatak, poput autentifikacijskih kodova koji se koriste u svrhu autorizacije transakcija (APPLI2/MAC ili APPLI3/MDS) ili da ponovite unos jednokratne lozinke nakon što ste sigurni da ste ju 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 internetsko bankarstvo putem nekog drugog kanala (elektroničke poruke, SMS-a i sl.) – ti podaci se koriste isključivo i samo na prijavnoj stranici HPB internetskog bankarstva.

Ukoliko uočite nepravilnosti molimo vas da ih **prijavite Banci 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 internetsko bankarstvo** uvijek je potrebno unijeti samo serijski broj tokena/mTokena i jednokratnu lozinku (APPLI1/OTP) – 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 HPB internetskog bankarstva za autorizaciju naloga potrebno je unijeti autorizacijski kod APPLI2/MAC ili APPLI3/MDS, a za dodavanje na Listu provjerenih primatelja APPLI3/MDS. Za radnje više razine rizika koje provodite putem HPB internetskog bankarstva, Banka primjenjuje snažnu ili pouzdana autentifikaciju klijenta, kako je detaljnije opisano kasnije u tekstu na primjeru APPLI3/MDS postupka. Kod APPLI3/MDS postupka prije potvrde naloga za plaćanje obvezno provjerite oba polja temeljem kojih se generira autentifikacijski kod (prvo polje mora odgovarati dijelu IBAN-a ili broja računa primatelja, a drugo iznosu transakcije s vodećim nulama). 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 web-stranice Banke (digitalni certifikat)** - prijavna stranica HPB internetskog bankarstva Banke ima ugrađen certifikat koji će vam potvrditi autentičnost stranice
- **Zaštita podataka u prijenosu** - pri prijenosu podataka koristi se TLS protokol. Svi podaci koje korisnik izmjenjuje s poslužiteljem HPB-a u svakom su trenutku šifrirani (kriptirani) uporabom tog protokola
- **Automatska odjava** - ako ste prijavljeni u HPB internetsko bankarstvo, ali ste određeno vrijeme neaktivni, biti ćete automatski odjavljeni
- **Onemogućivanje prijave** - nakon određenog broja neuspješnih pokušaja, prijava u HPB internetsko bankarstvo će Vam biti onemogućena
- **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 internetskog bankarstva
- **Snažna ili pouzdana autentifikacija korisnika u svrhu prijave** - kod pristupa HPB internetskom bankarstvu Banka primjenjuje **snažnu** dvofaktorsku autentifikaciju korisnika APPLI1/OTP. Pri tom je jedan faktor autentifikacije nešto što korisnik ima: token/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 APPLI2/MAC kod
- **Snažna ili pouzdana autentifikacija korisnika u svrhu autorizacije transakcije ili dodavanja na Listu provjerenih primatelja** - kako bi smanjila mogućnost zlouporabe 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 APPLI3/MDS autorizaciju unutar HPB internetskog bankarstva. Navedena autorizacija kod pokretanja postupka generiranja koda za autorizaciju, osim dvofaktorske autentifikacije, u svrhu **dodatne provjere s vaše strane**, zahtijeva unos dvaju polja koja su dinamički povezana s konkretnom transakcijom koju autorizirate. Kod primjera naloga za plaćanje, a prije potvrde s Vaše strane, obvezno provjerite dva važna polja duljine 8 znamenki koje Vas Banka traži kao unos: prvo mora odgovarati dijelu IBAN-a ili broju računa primatelja, a drugo mora odgovarati iznosu transakcije s vodećim nulama.

## 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 internetskog 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