

Sigurno korištenje m-zabom – mobilnim bankarstvom Zagrebačke banke



Vaša sigurnost iznimno nam je važna.

Saznajte kako se pravilno i sigurno koristiti uslugom m-zaba te kako zaštititi svoj mobilni uređaj.

- **Zaštitite svoj PIN za m-zabu**

Prilikom određivanja PIN-a za m-zabu odredite PIN koji je teško pogoditi. Za PIN nemojte odabrati datum rođenja, niz istih brojeva, npr. 111111 ili niz uzastopnih brojeva, npr. 123456. PIN kojim se koristite poznat je samo vama. Zapamtite ga i nemojte ga otkrivati drugim osobama ni zapisivati u mobitel, na računalo ili u druge bilješke. PIN m-zabe nemojte upotrebljavati za ostale mobilne aplikacije. Unosite svoj PIN isključivo prilikom prijave u svoju m-zabu. Ako smatrate da je druga osoba mogla steći uvid u vaš PIN, promijenite ga odmah putem m-zabe.

- **Zaštitite ključeve za aktivaciju m-zabe**

Nakon ugovaranja ili promjene m-zabe preuzet ćete ključeve za aktivaciju. Iskoristite ih i zatim uništite.

- **Odjavite se iz m-zabe**

Nakon završetka korištenja uslugom koristite se opcijom „Odjava“ u aplikaciji, osobito ako ostavljate mobilni uređaj bez nadzora.

- **Ne ustupajte m-zabu drugim osobama**

Ne prepuštajte drugim osobama da se koriste vašom m-zabom i nemojte instalirati m-zabu na mobilni uređaj druge osobe.

- **Ne dijelite pristupne podatke**

Ne dijelite aktivacijske ključeve ili aktivacijski QR kod ni sa kim. Isključiva svrha ovih podataka je aktivacija vaše m-zabe na vašem mobilnom uređaju.

- **Ažurirajte m-zabu i operativni sustav svojega mobilnog uređaja**

Redovito preuzimajte nove verzije m-zabe sa službenih trgovina (App Store, Google Play, App Gallery) te provjeravajte jesu li dostupne nove verzije operativnog sustava za vaš mobilni uređaj.

- **Obratite pozornost na SMS i MMS poruke te elektroničku poštu**

Ne odgovarajte na SMS, MMS i e-poruke nepoznatih i sumnjivih pošiljatelja, ne klikajte na linkove i ne preuzimajte datoteke iz njih. Banka vam dostavlja poruke samo unutar m-zabe i neće vam slati e-poruke ili SMS poruke s vašim povjerljivim podacima.

- **Promjena mobilnog uređaja**

Na novom uređaju preuzmite m-zabu iz ovlaštene trgovine i aktivirajte ju uz pomoć ključeva preuzetih od bankara u poslovnici Banke ili samostalno tako da u postavkama m-zabe na starom uređaju odaberete opciju Preseli m-zabu na novi uređaj. Ako se više ne koristite starim mobilnim uređajem, savjetujemo da ga vratite na tvorničke postavke i tako izbrišete podatke.

- **Čitajte poruke Banke i ostanite informirani**

Pratite objave o zaštiti podataka na javnim web-stranicama Banke i pročitajte obavijesti koje vam Banka dostavlja putem m-zabe i e-zabe. Informirajte se o mogućim prijevarama na web-stranicama Hrvatske udruge banaka ili Nacionalnog CERT-a.

- **Provjerite podatke na nalogu prije potvrde plaćanja**

Provjerite podatke na nalogu (posebno IBAN primatelja, iznos, datum izvršenja) prije provođenja naloga.

Napomena za poslovne subjekte: Povećajte oprez kad prvi put plaćate dobavljaču ili kad vas dobavljač obavijesti o promjeni svojeg IBAN-a / broja računa putem e-maila – svakako provjerite ispravnost IBAN-a drugim kanalom osim e-maila. Podaci o računima poslovnih subjekata u Republici Hrvatskoj javno su dostupni te predlažemo da provjerite je li naznačeni IBAN povezan s poslovnim subjektom u čiju korist se obavlja plaćanje.

- **Bluetooth i Wi-Fi**

Kako biste spriječili neovlašten pristup vašem mobilnom telefonu, savjetujemo da isključite Bluetooth i Wi-Fi kad se njima ne koristite.



- **Antivirusna zaštita za mobilne uređaje te aplikacije za praćenje uređaja**

Najčešći je uzrok zaraze virusom preuzimanje različitih aplikacija iz neovlaštenih trgovina. Antivirusna zaštita postoji za pojedine proizvođače mobilnih uređaja, a ako proizvođač softvera podupire antivirusnu zaštitu, preuzmite ju isključivo sa službenih trgovina (App Store, Google Play, App Gallery). Upoznajte se s upotrebom aplikacija putem kojih možete pratiti svoj uređaj u slučaju da dođe do njegova gubitka.

- **Redovito provjeravajte stanje i promete svojih računa**

Redovito (dnevno) provjeravajte stanje i promete po svojim računima u Banci i obratite nam se ako uočite sumnjive aktivnosti. Napomena za poslovne subjekte: Uvid u stanje i promete po računima ovisi o vrsti ugovorenog ovlaštenja.

- **Redovito ažurirajte svoje kontaktne podatke u Banci**

Redovito ažurirajte svoje kontaktne podatke (broj telefona, e-mail, poštansku adresu i drugo) putem e-poslovnice kojoj pristupate putem e-zabe, ili odlaskom u poslovnicu.



KAKO VAS BANKA ŠTITI?

- **Sigurnost rada m-zabe i zaštita podataka**

Svi podaci koji su razmjenjuju između m-zabe i Banke zaštićeni su kriptiranom vezom, a za pristup je potreban PIN. Podaci o PIN-u i računima ne čuvaju se u mobilnom uređaju. Aktivacijom m-bankarstva u mobilni uređaj instalira se softverski token koji jamči sigurnost korištenja uslugom.

- **Vaš PIN**

Unos PIN-a zaštićen je od neovlaštenog snimanja tipkovnicom s nasumičnim prikazom brojeva za unos PIN-a. Banka nema pristup vašem PIN-u i ne sprema ga, a PIN je poznat samo vama. Banka vas nikad neće zatražiti vaš PIN ili broj tokena/m-tokena! Također, Banka vas nikad neće tražiti unos PIN-a više od jednom.

- **Zaključavanje m-zabe i automatska odjava**

Nakon trostrukog uzastopnog unosa krivog PIN-a m-zaba se automatski zaključava. Ponovnu aktivaciju možete provesti kod bankara u poslovnici Banke ili telefonskim pozivom korisničkoj podršci za m-zabu na broj +385 1 3789 785. Također, nakon tri minute nekorištenja, m-zaba će vas automatski odjaviti.

- **Gubitak ili nestanak uređaja**

Za korištenje m-zabom potreban je PIN. Ako ga niste nigdje zabilježili ni povjerali drugim osobama, vaša je m-zaba sigurna čak i kad je uređaj izgubljen. No, da biste bili potpuno bezbrižni, prijavite nestanak uređaja Banci – odmah ćemo blokirati vašu m-zabu.

- **Sigurnost sustava**

Banka kontinuirano ulaže u unaprjeđenje sigurnosti sustava i usklađenost sa sigurnosnim standardima i preporukama regulatora. Banka redovito angažira neovisne stručnjake kako bi potvrdili sigurnost sustava.

Nikada nemojte...

- slati PIN za m-zabu e-mailom ili SMS-om,
- dijeliti aktivacijske ključeve ili aktivacijski QR kod m-zabe
- zapisivati svoj PIN u mobilni uređaj, na računalo ili u druge bilješke,
- koristiti se PIN-om m-zabe za druge aplikacije ili web-stranice,
- otvarati nesigurne web-stranice putem mobilnog uređaja,
- ostavljati osobne podatke i e-adrese na sumnjivim internetskim stranicama,
- preuzimati mobilne aplikacije s nepoznatih i neprovjerenih trgovina,
- koristiti se softverom mobilnog uređaja koji nije službeno izdan od proizvođača.

Obavijestite nas...

- ako izgubite mobitel ili vam ga ukradu,
- ako uočite sumnjive promete po svojim računima u Banci,
- ako zaprimite SMS, MMS i e-poruke sa sumnjivim sadržajem,
- ako primijetite nepravilnosti u radu vaše m-zaba aplikacije,
- ako smatrate da su druge osobe imale pristup vašoj m-zabi.

Korisnička podrška za m-zabu: +385 1 3789 785;
m-zaba@unicreditgroup.zaba.hr
Prijava gubitka ili krađe mobilnog uređaja: +385 1 3789 888