

Poštovani korisnici usluge CROBAnet Internet bankarstva,

Kako bi osigurali sigurnije korištenje usluge CROBAnet Internet bankarstva, preporučamo Vam da se pridržavate sljedećih sigurnosnih pravila:

**Održavanje i korištenje računala s kojeg pristupate usluzi CROBAnet Internet bankarstva:**

- *Pristup operativnom sustavu računala zaštitite snažnom zaporkom.*
- *Održavajte operativni sustav i aplikacije računala ažurnima, uvijek primjenjujući najnovije sigurnosne zakrpe proizvođača aplikacija i operativnog sustava.*
- *Koristite računalo kao standardni korisnik bez administratorskih privilegija.*
- *Zaštitite računalo aplikacijom za zaštitu od malicioznog koda, provodite redovna skeniranja sustava korištenjem iste te uključite automatsko osvježavanje zaštitnih definicija.*
- *Kako bi dodatno ograničili mogućnost neovlaštenog mrežnog pristupa Vašem računalu, uključite vatrozid mogućnost operativnog sustava računala.*
- *Aplikacije za računalo preuzimajte iz sigurnih i provjerenih izvora, po mogućnosti direktno s web stranica proizvođača aplikacije. Kad god je to moguće, koristite zadnju dostupnu verziju aplikacije.*
- *Ne otvarajte poruke elektroničke pošte od nepoznatih pošiljatelja te ne otvarajte poveznice ili privitke iz takvih poruka. Posebnu pozornost obratite na otvaranje privitaka, jer isti čak i unutar najčešće korištenih tipova datoteka (PDF, DOCX, XLSX i slične) mogu sadržavati maliciozni kod.*
- *Korištenjem dostupnih Vam mjera fizičke zaštite, zaštitite računalo od krađe, gubitka i neovlaštenog uvida u podatke, pogotovo u javnim prostorima.*
- *Preporuka je da usluzi CROBAnet Internet bankarstva ne pristupate s računala koja nisu pod Vašom kontrolom, javnih računala (hoteli, knjižnice, edukacijske ustanove i slično.) ili s računala koja koristi veći broj korisnika.*

**Korištenje Internet preglednika za pristup usluzi CROBANet Internet bankarstva:**

- *Koristite najnoviju dostupnu verziju Internet preglednika. Preporučeni Internet preglednici za pristup usluzi CROBANet Internet bankarstva su Google Chrome, Mozilla Firefox i Microsoft Internet Explorer.*
- *Vodite računa o drugim web stranicama koje posjećujete s računala putem kojeg pristupate usluzi CROBANet Internet bankarstva, jer neke stranice sumnjivog karaktera, kao što su stranice na kojima je moguće ilegalno preuzimanje aplikacija i ostalih sadržaja, stranice sa sumnjivim poslovnim ponudama te stranice za odrasle, povećavaju rizik od zaraze računala malicioznim kodom.*
- *Prije prijave na uslugu CROBANet Internet bankarstva, budite sigurni da se Vaš Internet preglednik nalazi na stvarnoj adresi web stranice usluge CROBANet Internet bankarstva <https://crobanet.croatiabanka.hr>. Adresa web stranice vidljiva je u adresnoj traci Vašeg Internet preglednika.*

*Preporuka je da ovu provjeru izvršite prilikom svakog pristupa usluzi CROBANet Internet bankarstva. U odnosu na stvarnu adresu, web adrese podmetnute od strane napadača mogu u svom nazivu imati samo jedno slovo, znak ili točku razlike te na prvi pogled mogu izgledati vrlo slično stvarnoj adresi web stranice usluge CROBANet Internet bankarstva. Primjeri naziva takvih web adresa su:*

*<https://crobanet.croatiabanka.cn>, <https://crobanet.croatiabanka.hr.cn>.*

- *Kako biste bili sigurni da je komunikacija s web poslužiteljem usluge CROBANet Internet bankarstva zaštićena i kriptirana korištenjem TLS sigurnosnog protokola, nakon što se web stranica otvori u Internet pregledniku, provjerite:*
  - *Nalazi li se u adresnoj traci Internet preglednika znak lokota.*
  - *Ispravnost i valjanost sigurnosnog certifikata koji jamči kako stranica pripada Croatia banci. Ispravnost i valjanost sigurnosnog certifikata možete provjeriti klikom na simbol lokota u adresnoj traci vašeg Internet preglednika. Unutar polja certifikata provjerite je li certifikat stvarno izdan za uslugu CROBANet Internet bankarstva te datum do kojeg je certifikat valjan.*

**Tajnost podataka i rad s uslugom CROBAnet Internet bankarstva:**

- Prilikom prijave u uslugu CROBAnet Internet bankarstva, koristite isključivo serijski broj dodijeljenog Vam hardverskog ili mobilnog tokena te jednokratnu zaporku (OTP) generiranu korištenjem istog. Prijava na sustav od Vas nikada neće zatražiti dodatnu autentifikaciju/autorizaciju putem generiranog MAC broja. Nemojte zaboraviti da se generirani MAC broj koristi ISKLJUČIVO u slučaju autorizacije naloga za plaćanje.
- Nikome ne otkrivajte podatke o generiranoj jednokratnoj zaporki (OTP) za pristup usluzi CROBAnet Internet bankarstva, generiranom MAC broju ili trenutnom PIN-u za korištenje dodijeljenog Vam hardverskog ili mobilnog tokena. Zaposlenici Croatia banke od Vas nikada neće tražiti podatak o PIN-u ili generiranom MAC broju.
- Usluga CROBAnet Internet bankarstva za svoj rad ne zahtjeva instalaciju dodatnih aplikacija. NIKADA ne instalirajte aplikaciju koja tvrdi da je na bilo koji način povezana s CROBAnet uslugom Internet bankarstva.
- Nakon prijave u uslugu CROBAnet Internet bankarstva, u korisničkim postavkama usluge upišite Vašu e-mail adresu te uključite mogućnost primanja e-mail obavijesti o prijavi u uslugu CROBAnet Internet bankarstva i izvršenim transakcijama.
- Pratite svoje transakcije. Ukoliko uočite bilo kakve nepravilnosti, iste bez odgađanja prijavite na broj telefona 01 2391 633 ili na e-mail adresu [crobanet@croatiabanka.hr](mailto:crobanet@croatiabanka.hr).
- Krađu ili gubitak identifikacijskog uređaja za prijavu u uslugu CROBAnet Internet bankarstva, bez odgađanja prijavite Croatia banci na broj telefona 01 2391 633 i na e-mail adresu [crobanet@croatiabanka.hr](mailto:crobanet@croatiabanka.hr). Više informacija o postupku prijave pronađite u Općim uvjetima korištenja CROBAnet Internet bankarstva dostupnim preko web stranica Banke i web stranica usluge CROBAnet Internet bankarstva.

*Pod identifikacijskim uređajem se smatra od Croatia banke dodijeljeni hardverski token ili mobilni uređaj s instaliranim mobilnim tokenom.*