Bezbednosne preporuke za upotrebu usluga mobilnog, telefonskog i elektronskog bankarstva

Poštovani klijenti,

Ovaj dokument sadrži osnovne preporuke za bezbedno korišćenje usluga mobilnog bankarstva Moja mBanka biznis, telefonskog bankarstva, kao i elektronskog bankarstva Moja eBanka biznis (u daljem tekstu: mobilno, telefonsko i elektronsko bankarstvo) od strane klijenata – pravnih lica i preduzetnika (u daljem tekstu: Korisnik). Neophodno je da se Korisnik pridržava ovih uputstava kako bi adekvatno zaštitio uređaje koje koristi za mobilno, telefonsko i elektronsko bankarstvo. Posebnu pažnju treba posvetiti zaštiti i pravilnoj upotrebi podataka i informacija koje su neophodne za korišćenje navedenih usluga.

Prilikom kreiranja PIN-a ili korisničkih kredencijala (korisničko ime i lozinka), nemojte koristiti trivijalne kombinacije koje bi mogle biti poznate drugim licima (npr. datumi rođenja članova porodice, brojevi telefona, lični i adresni podaci, imena kućnih ljubimaca i slično).

Zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika dužno je da čuva tajnost elemenata za potvrdu identiteta, kako oni ne bi došli u posed drugog lica. Čuvanje ovih podataka na mestu dostupnom drugim licima smatra se grubom nepažnjom Korisnika. Ukoliko zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika sumnja ili ustanovi da drugo lice ima informaciju o elementima za proveru i potvrdu identiteta, dužno je da odmah promeni navedene elemente. Ukoliko dođe do grube nepažnje, Korisnik snosi štetu nastalu zbog gubitka, neovlašćenog ili neodgovarajućeg korišćenja elemenata za potvrdu identiteta.

Zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika je dužno da se prilikom upotrebe usluga mobilnog, telefonskog i elektronskog bankarstva pridržava Pravila i ovih Bezbednosnih preporuka, kao i pisanih uputstava za Korisnike i uputstava koja su sastavni deo aplikacija. Korisnik snosi svu štetu nastalu zbog nepridržavanja Pravila i pisanih uputstava, koja se mogu preuzeti na internet stranici banke.

Redovno ažurirajte operativni sistem i aplikacije na Vašem uređaju i pridržavajte se bezbednosnih preporuka proizvođača.

Neophodno je da zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika na uređajima sa kojih će koristiti usluge mobilnog i elektronskog bankarstva, instalira odgovarajuće aplikacije. Aplikacije za mobilno bankarstvo banka objavljuje u zvaničnim prodavnicama proizvođača operativnih sistema, odnosno:

- za Android - Google Play store
- za iOS - Apple store
- za Huawei uređaje - AppGallery

Aplikaciji za elektronsko bankarstvo, Korisnik pristupa preko sajta Banke, odnosno direktno preko adrese https://rol.raiffeisenbank.rs/CorporateV4

U cilju unapređenja usluge mobilnog bankarstva, banka će povremeno objavljivati nove verzije navedenih aplikacija, pri čemu je obaveza Korisnika da na svojim uređajima izvrši ažuriranje aplikacija na najnoviju verziju.

U slučaju da primetite neuobičajeno ponašanje ili izgled aplikacije za mobilno i elektronsko bankarstvo, molimo Vas da odmah kontaktirate Kontakt centar Raiffeisen banke.

Preporučuje se da Korisnik aktivira bezbednosne funkcionalnosti koje nudi mobilni uređaj (na primer, zaključavanje ekrana uređaja nakon određenog perioda neaktivnosti i sl).

Preporučena je upotreba programa za zaštitu od zlonamernog softvera i virusa.

Nikada nemojte odgovarati na poruke u kojima se pošiljalac obraća u ime Raiffeisen banke ili u ime banke traži od Vas da dostavite neki od ličnih podataka. Molimo Vas da takav slučaj odmah prijavite na adresu abuse@raiffeisenbank.rs ili Kontakt centru Raiffeisen banke.

Ukoliko dođe do krađe ili gubitka Vašeg mobilnog uređaja, potrebno je da odmah obavestite Raiffeisen banku na telefon +381 11 3202 100.

Vodite računa o fizičkoj bezbednosti Vašeg mobilnog uređaja, posebno kada ste na putovanjima ili mestima gde se nalazi veliki broj ljudi (kao što su sajmovi, konferencije ili druga javna okupljanja).

Ukoliko mobilni uređaj podržava **upotrebu biometrijskih elemenata** (npr. otisak prsta) za otključavanje i/ili korišćenje aplikacije, preporučujemo da **ovaj način autorizacije ne koristite ukoliko su na uređaju memorisani biometrijski podaci drugih osoba**.

Budite obazrivi prilikom ustupanja mobilnog uređaja na korišćenje drugim osobama, s obzirom da neovlašćeno mogu sačuvati svoje biometrijske podatke na Vašem uređaju. **Preporučujemo da onemogućite snimanje dodatnih biometrijskih elemenata (dodatnog otiska prsta) bez korišćenja PIN-a ili ranije memorisanog biometrijskog podatka.**

Preporučujemo da pažljivo postupate prilikom Bluetooth povezivanja sa drugim uređajima i da isključite *Bluetooth* konekciju kada Vam nije potrebna.

Budite obazrivi kada Vaš uređaj povezujete na napajanje drugih lica (kao što su tuđi desktop ili *notebook* računari ili stanice za dopunu mobilnih uređaja na javnim mestima). Povezivanjem mobilnog uređaja na port za napajanje može se pod određenim uslovima i bez Vašeg znanja pristupiti podacima i aplikacijama na uređaju.

Elemente korisničkog naloga i PIN za uslugu mobilnog, telefonskog i elektronskog bankarstva **nemojte saopštavati drugim licima.**

Nemojte čuvati osetljive podatke (kao što su lozinke, brojevi bankovnih računa, platnih kartica i slično) **na Vašim mobilnim uređajima.**

Korisnik je dužan da odmah zatraži blokadu mToken-a u svim slučajevima gubitka ili postojanja sumnje da su ovi podaci došli u posed neovlašćenog lica. Gubitak ili krađu kredencijala, mToken-a, tj. mobilnog telefona ili drugog mobilnog uređaja koje koristi za mobilno, telefonsko i elektronsko bankarstvo, kao i slučajeve narušavanja bezbednosti, Korisnik je u obavezi da prijavi banci na broj +381 11 3202 100, elektronskom poštom na adresu abuse@raiffeisenbank.rs ili lično u ekspozituri banke. Banka će odmah postupiti po prijavi Korisnika i/ ili Ovlašćenog lica Korisnika i u zavisnosti od zahteva, banka može blokirati mToken ili deaktivirati prijavljeni broj mobilnog telefona za dalju upotrebu mobilnog, telefonskog i elektronskog bankarstva. mToken se blokira od strane banke po prijemu obaveštenja na neki od prethodno navedenih načina. Korisnik će snositi eventualne posledice zloupotrebe mToken-a (PIN-a), odnosno podataka koji definišu korisnički nalog, nastale usled njegove namere ili grube nepažnje.

Blokirani mToken može se deblokirati na zahtev Korisnika u pisanoj formi. Deblokirani mToken se može koristiti na istom ili na drugom mobilnom uređaju Ovlašćenog lica. Troškove deblokade mTokena snosi Korisnik.

U slučaju neovlašćenog korišćenja mToken-a ili korisničkog naloga, Korisnik je dužan da odmah obavesti banku usmeno, a potom i u pisanoj formi, u roku od 3 dana od dana usmenog obaveštenja. Ovlašćeno lice je dužno da čuva tajnost korisničkog naloga i PIN-a, kako ne bi došli u posed neovlašćenih lica. Ukoliko zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika sumnja ili ustanovi da je neko saznao kredencijale, PIN ili lozinku, zakonski zastupnik i/ili ovlašćeno lice od strane Koirsnika može samostalno promeniti ove elemente preko aplikacije za elektronsko, odnosno mobilno bankarstvo. Zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika je u obavezi da čuva tajnost elemenata za potvrdu identiteta. Ukoliko ne postupi u skladu sa navedenim, Korisnik će snositi eventualne posledice zloupotrebe.

U slučaju da zakonski zastupnik i/ili lice ovlašćeno od strane Korisnika više puta zaredom unese pogrešne elemente za potvrdu identiteta, sigurnosni mehanizam će, u skladu sa poslovnom politikom banke, privremeno ili trajno blokirati zaštićene podatke i onemogućiti korišćenje usluge mobilnog, telefonskog i/ili elektronskog bankarstva.

Korisnik je odgovoran za tačnost svih podataka u nalogu za prenos, te snosi rizik unosa netačnih podataka.

Korisnik je odgovoran za tačnost svih podataka datih banci i obavezan je da prijavi svaku promenu tih podataka. Ukoliko banka samostalno ili iz drugih izvora informacija dođe do saznanja da su podaci o Korisniku netačni ili izmenjeni, može uskratiti dalje korišćenje usluge mobilnog, telefonskog i elektronskog bankarstva.

Dodatne bezbednosne preporuke možete pogledati na internet stranici Udruženja banaka Srbije (https://www.ubs-asb.com/)