e-ba

Sigurnosne preporuke

Vaša sigurnost nam je bitna! Saznajte kako se pravilno i sigurno koristiti e-ba uslugom.

Pristupanje e-ba usluzi

1. E-ba usluzi pristupate izravno sa službene web stranice

E-ba usluzi pristupajte izravno putem službene web-stranice Banke www.unicredit.ba, odabirom opcije "PRIJAVA U INTERNET BANKARSTVO -> E-BA (FIZIČKE OSOBE)“, a nikad putem linkova iz e-mailova ili s drugih web-stranica.

2. Za prijavu u e-ba uslugu potrebno je unijeti samo serijski broj tokena i jednokratnu lozinku (APPLI1/OTP)

Ako se za prijavu od Vas traži neki drugi podatak, poput podatka za autorizaciju transakcije (APPLI2/MAC), ili još jedna jednokratna lozinka, prekinite prijavu i odmah to prijavite Banci. Banka od Vas nikad neće tražiti jednokratnu lozinku (APPLI1/OTP) ili podatak za autorizaciju transakcije (APPLI2/MAC) kako bi potvrdila Vaše podatke, ponovo registrirala Vaš token i slično. Također, Banka od Vas nikad neće tražiti dostavu podataka za prijavu u e-ba uslugu putem nekog drugog kanala (e-maila, SMS-a i slično).

3. APPLI2/MAC unosite samo nakon što ste se prijavili u e-ba

APPLI2/MAC unosite samo kad ste prijavljeni u e-ba uslugu, nakon što ste putem e-ba usluge zadali nalog/transakciju koju je potrebno autorizirati tokenom.

Zaštitite svoje podatke

1. Obratite pozornost na elektroničku poštu

Molimo obratite pozornost na e-mailove koji stvaraju privid dolaska od UniCredit Banke (npr. e-adresa pošiljatelja stvara privid e-adrese Banke, npr. u sadržaju e-maila nalazi se logo UniCredit Banke i slično), a sadržavaju linkove i privitke te gramatički neusklađene rečenice.

- Ne odgovarajte na takve e-mail poruke, ne klikajte na linkove i ne otvarajte privitke iz takvih poruka.
- Na e-ba uslugu ulazite isključivo izravno s web-stranica Banke, a ne putem linkova iz e-mail poruka ili drugih web stranica.
- Banka Vam nikad neće slati e-mailove u kojima Vas poziva da kliknete na link kako biste pristupili e-ba usluzi.
- Banka Vam dostavlja obavijesti unutar e-ba usluge, neće Vam poslati e-mail kako bi Vam javili da imate poruku u e-ba usluzi.

2. Što trebate izbjegavati, tj. nikada ne činiti

- Otvaranje e-maila za koji niste sigurni tko je pošiljatelj (sumnjiv nazivi poruke, sumnjiv pošiljatelj ili poruke poslane “samom sebi”). Pogotovo nemojte otvarati linkove ili privitke iz njega.
- Slanje PIN-a ili podataka za prijavu u e-ba uslugu putem e-maila.

UniCredit Bank

• Otvaranje nesigurnih i sumnjivih stranica.

• Pokretanje sumnjivih programa.

• Instaliranje dodatnih programa za rad na e-ba usluzi. Banka od Vas nikada neće tražiti instalaciju dodatnog programa za rad e-ba usluge. U tu svrhu nikad Vam neće poslati e-mail s programom u prilogu ili linkom koji upućuje na web-stranicu s koje biste trebali preuzeti takav program.

• Ostavljanje osobnih podataka i e-mail adrese na sumnjivim stranicama.

3. Zaštitite svoj PIN i OTP/MAC

Pouzdanost identifikacije ovisi o dostupnosti parametara za identifikaciju (broja tokena i OTP-a) samo ovlaštenom korisniku, stoga:

• ne otkrivajte nikome svoj PIN za token ili m-token i ne držite PIN uz token ili m-token,

• birajte PIN koji je teško pogoditi (ne upotrebljavajte npr. „1234“ ili datum rođenja),

• podatke poput broja tokena i PIN-a za token ne pohranjujte na računalu, jer ako kriminalci zaraze Vaše računalo, doći će u posjed svih podataka na njemu, uključujući i Vaše povjerljive podatke.

Napominjemo da zaposlenici Banke nikad neće tražiti od Vas odavanje povjerljivih podataka kao što su prethodno navedeni (PIN i slično), stoga molimo da ih nikad ne odajete trećim osobama putem telefona, e-maila, računala ili na druge načine.

4. Čitajte obavijesti Banke

Pratite obavijesti koje Vam Banka dostavlja putem e-ba usluge.

5. Provjerite podatke na nalogu prije potvrde plaćanja

Provjerite podatke na nalogu (broj računa primatelja/IBAN, iznos i poziv na broj) prije provođenja naloga (slanja naloga na plaćanja).

6. Redovito ažurirajte svoje kontaktne podatke

Redovito ažurirajte svoje kontaktne podatke u Banci (broj telefona, e-mail, poštansku adresu i drugo).

7. Redovito provjeravajte stanje i promete po svojim računima

Redovito provjeravajte stanje i promete po svojim računima kako biste što prije uočili sumnjive aktivnosti. Ako uočite bilo kakvu sumnjivu aktivnost, odmah ju prijavite Banci.

8. Odjavite se

Nakon prestanka rada u e-ba usluzi odmah se odjavite klikom na gumb „**Odjava**“.

Ako posumnjate na prevaru ili bilo kakvu sumnjivu aktivnost, odmah obustavite rad na računalu te prijavite slučaj na besplatan info broj **080 081 051** (za pozive iz inozemstva ++ 387 33 567 460) ili na **eba.gradjani@unicreditgroup.ba**

Zaštitite svoje računalo

1. Redovito održavajte svoje računalo

Sigurnost Vaših podataka ovisi i o zaštiti Vašeg računala od virusa i drugih zlonamjernih programa koji mogu doći u posjed Vaših parametara za identifikaciju ili autorizaciju naloga za plaćanje. Za pristup e-ba usluzi koristite se samo računalima s ažuriranom programskom potporom. Savjetujemo da ne pristupate e-ba usluzi s neprovjerenih računala ili računala kojima se koristi više osoba poput računala u web caffe-u. Održavanje računala treba obuhvatiti redovito ažuriranje operativnog sustava, internetskog preglednika, antivirusnog i antispyware programa te ostalih aplikacija kojima se koristite, zadnjim zakrpama proizvođača.

2. Uključite antivirusnu zaštitu i vatrozid

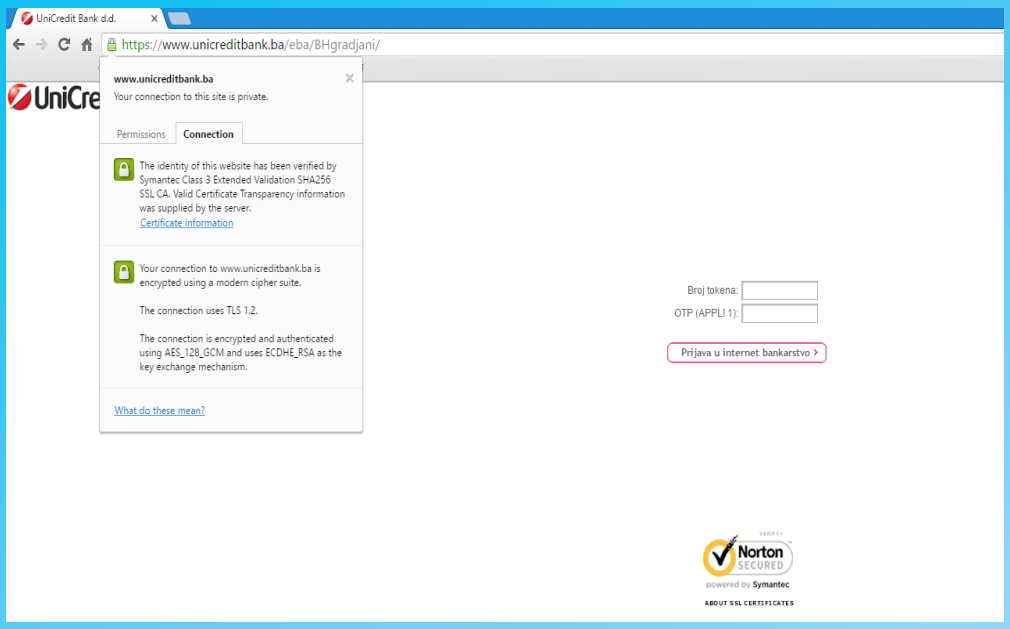
Obvezno uključite antivirusnu zaštitu i osobni vatrozid na svojem računalu. Redovito ažurirajte antivirusnu zaštitu te provodite redovito skeniranje računala na viruse i druge maliciozne programe, npr. jednom tjedno.

UniCredit Bank

Kako Vas Banka štiti?

1. Provjera autentičnosti web-stranice Banke

Provjerite nalazite li se na stranici koja pripada Vašoj Banci, to možete provjeriti i klikom na lokot u adresnom polju. Banka primjenjuje certifikat izdan od renomiranog izdavatelja certifikata (Symantec). Provjeru provedite prije prijave u e-ba uslugu.



2. Zaštita podataka u prijenosu

Podaci u prijenosu između Vašeg računala i Banke zaštićeni su kriptiranjem veze. Ostvarena vrsta enkripcije veze najviša je moguća koju podupire Vaš internetski preglednik. Da je enkripcija ostvarena, možete provjeriti ako adresa stranice počinje s https i ako se u adresnom polju ili u statusnoj traci (ovisno o vrsti Vašeg internetskog preglednika) nalazi lokot.

3. 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.

4. Automatska odjava

Ako ste prijavljeni u e-ba uslugu i neko se vrijeme njome ne koristite, nakon određenog vremena Banka će Vas automatski odjaviti iz e-ba usluge kako bi smanjila mogućnost pristupa neovlaštene osobe Vašim računima i podacima.

5. Onemogućivanje prijave

Ako netko pokuša pogoditi Vašu jednokratnu lozinku (One time password – OTP), nakon određenog broja neuspješnih pokušaja prijava u e-ba uslugu bit će onemogućena.

6. Praćenje internetskih prijetnji

Banka redovito prati pojavu novih internetskih prijetnji i provjerava sigurnost usluge na nove prijetnje.

7. Objave o sigurnosnim prijetnjama

Kako bi Vas upozorila na pojavu novih prijetnji i postupaka koje implementira da bi Vas zaštitila, Banka Vam ostavlja obavijesti na svojoj javnoj web stranici i unutar e-ba usluge.

8. Identifikacija korisnika

Identificirajući korisnika putem dvofaktorske autentifikacije (onoga što korisnik ima – token ili m-token i onoga što korisnik zna – PIN) prilikom pristupa e-ba usluzi Banka želi osigurati pristup samo ovlaštenom korisniku.

9. Autorizacija naloga za plaćanje

Banka će od Vas tražiti podatke za autorizaciju (APPLI2/MAC) samo kada provodite nalog za plaćanje.

UniCredit Bank