SLATINSKA BANKA

SIGURNOST USLUGE INTERNET BANKARSTVA SLATINSKE BANKE D.D.

Internet bankarstvo Slatinske banke d.d. je usluga koja omogućava, uz pomoć osobnog računala s pristupom Internetu, 24 sata dnevno pristup do računa u banci. Uslugom Internet bankarstva omogućen je uvid u trenutna stanja i promete po transakcijskim računima, obavljanje i pregled financijskih transakcija, kupoprodaju valuta, primanje izvadaka o stanju i prometu po transakcijskim računima, različitih obavijesti, te autoriziran način komunikacije s bankom.

Opasnosti korištenja Interneta

Napredak tehnologije, 24 satna dostupnost usluge, te sve sofisticiraniji maliciozni softver omogućila je i zloupotrebu usluge Internet bankarstva na razne načine:

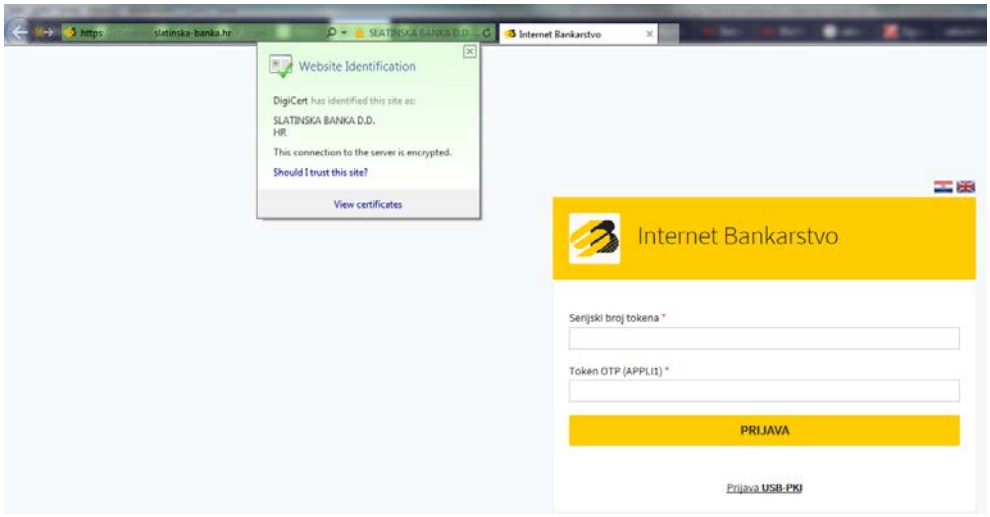
- ***Phishing*** - je proces putem kojega zlonamjerne osobe dobivaju pristup osjetljivim podacima poput korisničkih imena, lozinki ili podataka s kreditnih kartica, slanjem lažnih elektroničkih ili tekstualnih poruka koje izgledaju kao da su ih poslale legitimne organizacije.
- ***Vishing*** - je sličan phishingu, ali se odnosi na lažne telefonske pozive u kojima se prevaranti predstavljaju kao zaposlenici banke ili druge poznate organizacije, te Vas tražiti da novac s vlastitoga računa prebacite na neki nepoznati račun.
- ***Malware*** - je zajednički naziv za štetne ili maliciozne programe (virusi, trojanci, spyware/ adware, …) koje zlonamjerne osobe koriste kako bi pristupili Vašem računalu. Takvi su programi obično skriveni u privicima ili besplatnom sadržaju.
- ***Spam*** - je neželjena e-poruka koju zlonamjerne osobe šalju na milijune i u kojima tvrde da predstavljaju financijske institucije. Njihove e-poruke sadrže privitke u kojima se navodno nalaze podaci o, primjerice, sumnjivoj transakciji, račun, faks ili glasovna poruka.

Sigurnost – korisnik

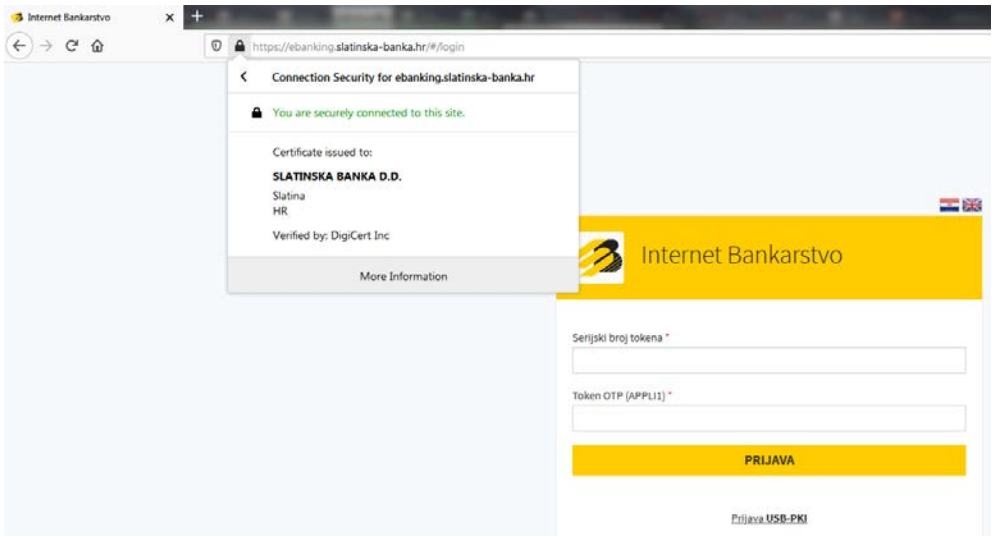
1. ***Pristupanje Internet bankarstvu***
   Internet bankarstvu Slatinske banke pristupajte izravno putem službene web-stranice Banke www.slatinska-banka.hr, odabirom opcije „Internet bankarstvo“, a nikad putem linkova iz e-mailova ili s drugih web-stranica.

2. ***Provjera službenih stranica Banke***
   Prije prijave u Internet bankarstvo Banke provjerite nalazite li se zaista na stranici Banke, a što možete na sljedeće načine:
   a) u adresnom polju, klikom na lokot, ovisno o pretraživaču kojim se koristite, ovakav prikaz trebate vidjeti:

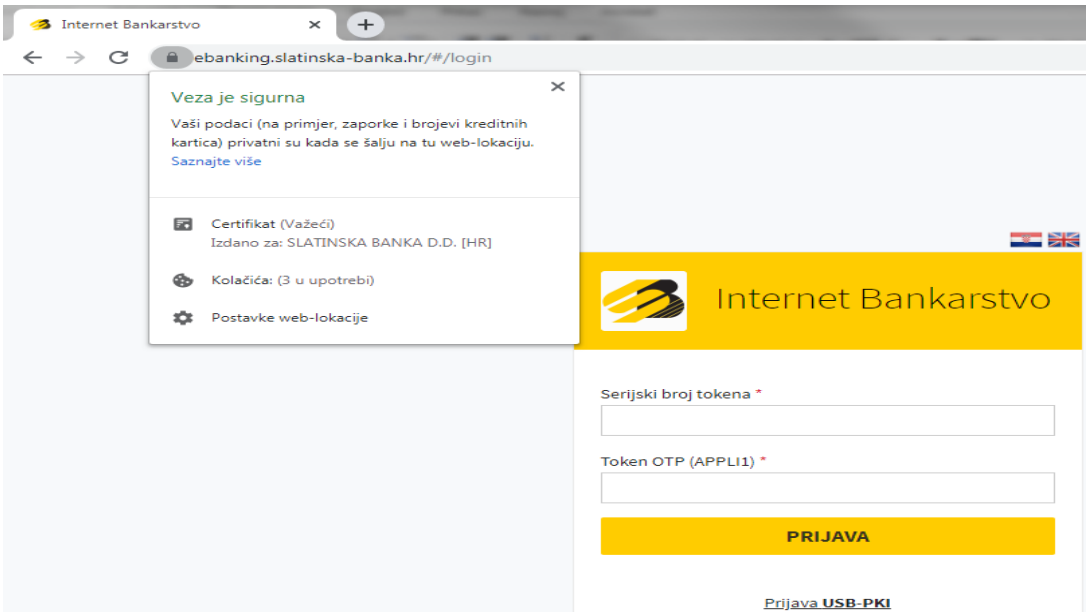
Internet Explorer



Google Chrome



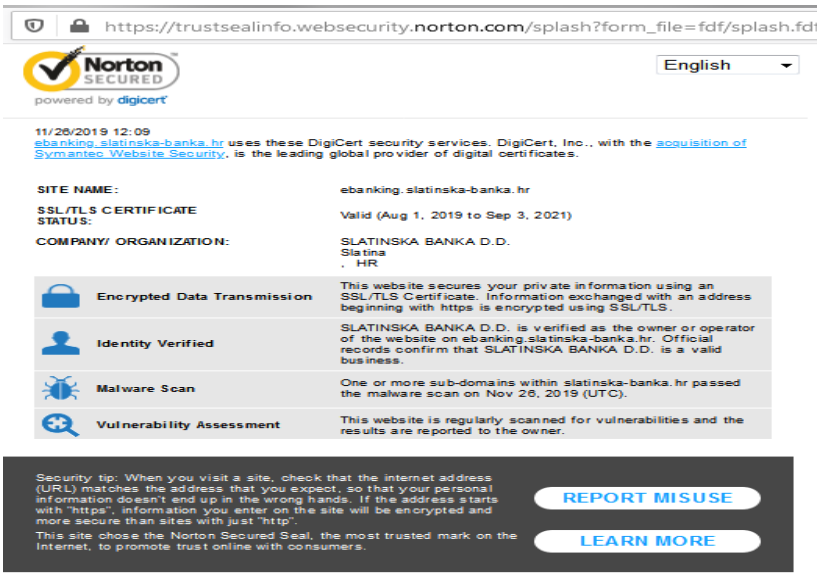
Mozilla Firefox



b) klikom na pečat tvrtke Norton.

Pečat treba izgledati ovako:

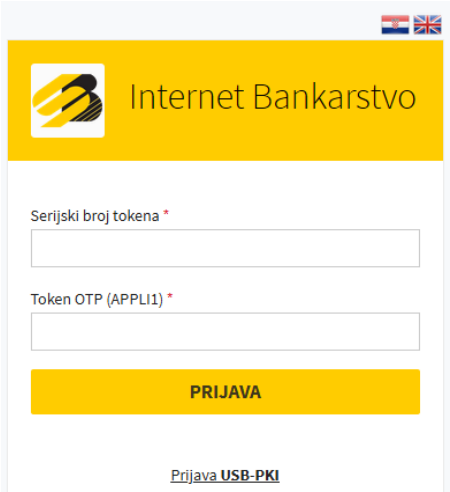
Potvrda autentičnosti stranice treba izgledati ovako:



3. *Prijava na Internet bankarstvo Banke*

Prilikom prijave na uslugu Internet bankarstva Banke identifikacija korisnika zasniva se na uporabi USB PKI uređaja s certifikatom FINA-e i PIN-a (pravne osobe), te serijskog broja tokena (pravne i fizičke osobe) i jednokratne lozinke (APPLI1). Identificirajući korisnika Banka provjerava da li je osoba koja se prijavljuje na uslugu Internet bankarstva Banke stvarni, za to ovlašteni korisnik, a sam korisnik istovremeno je osiguran da nitko drugi nema pristup njegovim računima i sredstvima.

Primjer ispravnog izgleda ekrana za prijavu u Internet bankarstvo Banke:



Obustavite rad na računalu ako primijetite da ekran za prijavu u Internet bankarstvo Banke ne izgleda ovako.

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

4. *Autorizacija naloga*

APPLI2 unosi se samo kad ste unutar usluge Internet bankarstva banke i to nakon što ste zadali nalog/transakciju koju je potrebno autorizirati tokenom.

5. *Minimalni tehnički zahtjevi*

Za korištenje Internet bankarstva, a u cilju povećanja sigurnosti, dužni ste ispuniti sljedeće minimalne tehničke zahtjeve:

- Operativni sustav - Windows 7
- Novije verzije Internet preglednika podržani od strane proizvođača - Internet Explorer, Firefox, Google Chrome

6. *Sigurnosne preporuke*

Za korištenje Internet bankarstva nužno je pridržavati se sljedećih sigurnosnih preporuka:

- Koristiti kvalitetne antivirusne, anti-spyware i anti-spam programe. Programe redovno ažurirati i periodično pokretati skeniranje računala.
    - Licencirani korisnici operativnog sustava Microsoft Windows imaju pravo besplatnog korištenja Microsoft antivirusnog programa:
      http://www.microsoft.com/security/portal
    - Popis ostalih proizvođača Windows antivirusnog programa:
      http://windows.microsoft.com/en-US/windows/antivirus-partners
- Redovno ažurirati operativni sistem, web preglednike i instalirane programe novim sigurnosnim nadogradnjama.
- Koristiti pravilno konfiguriran osobni vatrozid program koji sprječava pristup internoj mreži i računalu.
- Po završetku rada, odjaviti se iz Internet bankarstva i ukloniti iz računala USB PKI uređaj za prijavu. U slučaju duže neaktivnosti biti će te automatski odjavljeni sa stranica Internet bankarstva.
- Ne čuvati USB PKI ili token i njihove PIN-ove na istom mjestu.
- Kao PIN ne koristiti jednostavne kombinacije (npr. 1234, 1111,2222,1122, datum rođenja …)
- Ne otkrivati tajne podatke koji se koriste za Internet bankarstvo. Banka nikada neće tražiti da se tajni podaci dostavljaju e-poštom, SMS-om, telefonom ili na neki drugi način.
- Stranicama Internet bankarstva nužno je pristupati preko glavne Internet stranice Banke ili linka kreiranog preko glavne stranice Banke (nikako klikom na link iz pošte nepoznatog pošiljatelja).
- Ne otvarajte e-poštu za koji niste sigurni tko je pošiljatelj.

  Primjeri e-pošte koji spadaju u kategoriju SUMNJIVO:
    - ✓ e-pošta od nepoznatog pošiljatelja ili pošiljatelja od kojeg ne očekujete e-poštu
    - ✓ brojevi u nazivu e-pošte
    - ✓ e-pošta pisana na lošem hrvatskom jeziku ili stranom jeziku
    - ✓ zamolba da se otvori datoteka iz priloga (npr. ZIP, PDF, …) ili da se otvori link iz e-pošte

- ✓ e-pošta koja se „čini“ da je od poznatog pošiljatelja - korištenje domena sličnog imena
  - jedinstveno ime/adresa (domena) Banke na Internetu je „**slatinska-banka.hr**“
- ✓ e-pošta koja Vas pokušava navesti na otkrivanje povjerljivih osobnih podataka (korisnička imena i zaporke, PIN brojevi, brojevi kreditnih kartica i sl.)

7. ***Informirajte se***
   Redovito se informirajte o mogućim prijevarama i savjetima putem web-stranice Hrvatske udruge banaka: (https://www.hub.hr/hr/sigurnost-na-internetu/savjeti-za-gradane/sigurnost-racunala-i-internet-bankarstva) ili na web-stranicama Anti-Botnet Nacionalnog centra potpore (http://www.antibot.hr/index).

8. ***Čitajte poruke Banke***
   Pratite objave o zaštiti podataka na javnim web-stranicama Banke i pročitajte obavijesti koje Vam Banka dostavlja putem Internet bankarstva Banke.

9. ***Provjerite podatke na nalogu prije potvrde plaćanja***
   Provjerite podatke na nalogu (IBAN ili broj računa primatelja, iznos i poziv na broj) prije provođenja naloga (zadavanja plaćanja).

10. ***Redovito ažurirajte svoje kontaktne podatke***
    Redovito osvježujte svoje kontaktne podatke kod Banke (broj telefona, e-mail, poštansku adresu i drugo).

11. ***Redovito provjeravajte stanje i promete po svojim računima***
    Redovito provjeravajte stanje i promete po svojim

12. ***Prijava zloupotrebe***
    U slučaju sumnje na prijevaru, zlouporabe korisničke identifikacije ili gubitka uređaja odmah obavijestite Banku:

    Sektor platnog prometa
    Telefon: 033/637-033
    radno vrijeme: od 08:00 do 17:00 sati svakog radnog dana
    e-mail: internet-bankarstvo@slatinska-banka.hr

    Sektor IT-a
    Telefon: 033/637-072
    Radno vrijeme: od 07:00 do 20:00 sati svakog radnog dana, a subotom od 08:00 do 13:00 sati
    e-mail: internet-bankarstvo@slatinska-banka.hr

13. ***Blokiran USB PKI ili token***
    U slučaju da je Vašom greškom blokiran USB PKI ili token uređaj vlasnik uređaja ili ovlaštena osoba dužna je osobno obratiti se najbližoj poslovnici Banke kako bi se uređaj otključao.

Sigurnost – Banka

Banka primjenjuje najnovije sigurnosne standarde, te neprekidno radi na njihovom unaprjeđivanju kako bi osigurala da se na siguran način obavljaju transakcije koristeći web aplikaciju Internet bankarstvo.

Sigurnost stranice Internet bankarstva, te komunikacije između korisnika i web servera Internet bankarstva osigurana je korištenjem:

1. ***Certifikata***

   Kako bi bili sigurni da komunicirate s poslužiteljem (serverom) Internet bankarstva Banke koristi se Extended Validation certifikat izdan od tvrtke DigiCert kojim se potvrđuje identitet Banke.

   Naziv poslužitelja naveden u zelenom adresnom polju Internetskog pretraživača mora u svakom trenutku biti identičan onom navedenom u certifikatu – „**ebanking.slatinska-banka.hr**“.

2. ***Pečat (Seal)***

   Norton Trust pečat jamči Vam sigurnost i povjerenje u stranicu Internet bankarstva Banke.

   Klikom na ikonu može vidjeti da je Banka osigurana i podržana od strane tvrtke DigiCert. Važna funkcija Norton Trust pečata je i svakodnevno provjeravanje web stranica od malicioznog koda (virusa, raznih vrsta prijevara, ...).

3. ***SSL enkripcije***

   Prilikom posjete na Internet bankarstvo Banke komunikacija se uspostavlja putem sigurne SSL veze. Svaki podatak koji se pošalje ili primi od Banke je šifriran, što osigurava da samo Vi može pročitati svoje podatke.

4. ***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.

5. ***Automatska odjava***

   Ako ste prijavljeni u Internet bankarstvo Banke, nakon određenog vremena neaktivnosti Banka će Vas automatski odjaviti iz Internet bankarstvo Banke kako bi smanjila mogućnost pristupa neovlaštene osobe Vašim računima i podacima.

6. ***Sigurnost transakcije***

   Sigurnost provođenja transakcije Internet bankarstva osigurana je postojanjem više sigurnosnih mjera (globalna lista, bijela lista, neuobičajena transakcija), a u ovisnosti o visini transakcije i ukupnog dnevnog zbroja iznosa svih transakcija primjenjuju se dodatne sigurnosne postavke pri autorizaciji naloga (Limiti).

7. ***Blokiranje usluge Internet bankarstva***

   Ako netko pokuša pogoditi Vašu jednokratnu lozinku (One time password – OTP), nakon određenog broja neuspješnih pokušaja prijava usluga Internet Bankarstva biti će onemogućena.