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.

Napredak tehnologije, 24 satna dostupnost usluge, te niska svijest korisnika o sigurnosti 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 od korisnika traže 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 korisničkim računalima. 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

Prilikom prijave na uslugu Internet bankarstva Slatinske banke identifikacija korisnika zasniva se na uporabi USB PKI uređaja s certifikatom FINA-e (pravne osobe) i tokena (pravne i fizičke osobe), te njihovih PIN-ova. 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.

Za korištenje Internet bankarstva, a u cilju povećanja sigurnosti, korisnik je dužan ispuniti sljedeće minimalne tehničke zahtjeve:

- Operativni sustav - Windows 7
- Novije verzije Internet preglednika - Internet Explorer

Za korištenje Internet bankarstva nužno je da se korisnik pridržava 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 (10 minuta) korisnik će biti automatski odjavljen sa stranica Internet bankarstva.
- Ne čuvati USB PKI ili token i njihove PIN-ove na istom mjestu.

- Ne otkrivati tajne podatke koji se koriste za Internet bankarstvo. Banka nikada neće tražiti da se tajni podaci dostavljaju e-poštom, telefonom ili na drugi nesiguran 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).

Gubitak ili krađa Uređaja
U slučaju zlouporabe korisničke identifikacije ili gubitka uređaja klijent je dužan odmah obavijestiti Banku:

- **Sektor platnog prometa**
  Telefon: 033/637-033
  radno vrijeme: do 17:00 sati svakog radnog dana
  e-mail: internet-bankarstvo@slatinska-banka.hr
  ili
- **Sektor IT-a**
  Telefon: 033/637-072
  Radno vrijeme: do 21:00 sati svakog radnog dana, a subotom do 13:00 sati
  e-mail: internet-bankarstvo@slatinska-banka.hr.

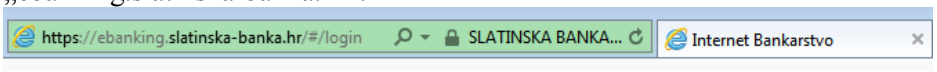
Blokiran USB PKI ili token
U slučaju da je korisničkom greškom blokiran USB PKI ili token uređaj vlasnik uređaja ili ovlaštena osoba dužna je osobno obratiti se najbližoj poslovnici Banke kako bi se uređaj otključao.

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:

- **Certifikata**
  Kako bi korisnik bio siguran da komunicira s poslužiteljem (serverom) Internet bankarstva Banke koristi se „secure site pro extended validation“ certifikat izdan od tvrtke Symantec kojim se potvrđuje identitet Banke. Javni ključ certifikata je dužine 2048Bita, potpisni algoritam je sha256RSA. Naziv poslužitelja naveden u zelenom adresnom polju Internetskog pretraživača mora u svakom trenutku biti identičan onom navedenom u certifikatu – „ebanking.slatinska-banka.hr“.



- **Seal-a**
  Verisign Trust Seal jamči posjetitelju sigurnost i povjerenje u stranicu Internet bankarstva Banke. Korisnik klikom na ikonu može vidjeti da je Banka osigurana i podržana od strane tvrtke Verisign. Važna funkcija Verisign Trust seal-a je i svakodnevno provjeravanje web stranica od malicioznog koda (virusa, raznih vrsta prijevara, ...).

- **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 korisnik može pročitati svoje podatke.

Sigurnost stranica Internet bankarstva osigurana je modernim sigurnosnim tehnikama, te se dodatno redovito provjerava sigurnosnim alatima.

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**).