Poštovani,

Želimo Vam ugodno korištenje Internet bankarstva za pravna lica. Internet bankarstvo kvalitetan je alat koji trebate pažljivo koristiti kako biste izbjegli eventualne poteškoće i uživali u njegovom korištenju. Sigurnost sistema ali i poslovanja u cjelini osnovni je postulat naše poslovne politike. Kontinuirano unapređenje sigurnosnih aspekata naš je prioritet.

Informacije koje podijelite sa bankom ne mogu se zloupotrijebiti po bilo kojem osnovu, niti iskoristiti u bilo koju svrhu osim one za koju su date. Svi Vaši podaci čuvaju se i tretiraju u skladu sa važećim zakonima i drugim propisima koji regulišu ovu oblast.

Vaši identifikacioni podaci su Vaši privatni podaci koje Vam niko nikada neće tražiti, niti ste bilo kome dužni dati te podatke. Isto se odnosi na broj Vašeg računa ili kartice.

Edukacija korisnika je osnovni, a često i jedini način suzbijanja prevara putem Interneta, stoga ćemo Vas, u cilju prevencije prevara i zaštite Vaših podataka, u nastavku upoznati sa mogućim pokušajima prevare putem e-maila/Interneta i mjerama za unapređenje sigurnosti.

Mjere za dodatno unapređenje sigurnosti Vašeg poslovanja

- Molimo Vas da vodite računa o sljedećem:
- Trebate čuvati identifikacioni broj, statičku lozinku i token na sigurnom.
- Ako ste u u sumnji da je neko saznao Vašu osobnu šifru (PIN) odmah ste je dužni promijeniti. Informacije o promjeni šifre možete dobiti:
  - putem telefona + 387 33 28 78 90, 28 78 91, 28 78 92, 28 78 93 (radnim danom od 08:30 do 16:30) kako bi se blokirao servis
  - putem e-mail adrese: support.desk@rbb-sarajevo.raiffeisen.at.
  - na web stranici: www.raiffeisenbank.ba
- Ako ste u sumnji da bi neko mogao zloupotrijebiti Vaš pristup servisu potrebno je da odmah nazovete Raifeisen direkt info: + 387 33 75 50 10.
- Na kraju rada kliknite na "Izlaz".

Mjere koje preporučujemo:

- Instalirajte ažuran antivirusni program.
- Radite sedmično skeniranje vašeg računara zbog virusa i spywarea.
- Instalirajte privatni ili hardverski firewall.
- Ne dijelite Vašu osobnu šifru (PIN) ni sa kim.
- Ne koristite Internet bankarstvo sa javnih ili nesigurnih računara.
- Ne ostavljajte naljepnice sa vašim identifikacijskim podacima na računaru ili oko računara.
- Ne ostavljajte u računaru dokumente koji sadrže vaše identifikacijske podatke.
- Ne skidajte programe sa sumnjivih stranica.
- Ne otvarajte e-mailove sumnjivih sadržaja.
- Pazite se lažnih e-mailova koji mogu izgledati kao da ih je poslala Raiffeisen banka – detaljnije o *phishingu* u nastavku:

Veoma čest pokušaj prevare je tzv. ***phishing,*** koji predstavlja pokušaj iznuđivanja povjerljivih podataka od korisnika Interneta, kao što su korisnička imena, lozinke i podaci o karticama, s ciljem zloupotrebe istih.

Phishing se provodi putem falsifikovane web stranice koja se lažno predstavlja kao npr. stranica za online plaćanje, banka ili npr. popularna društvena web stranica i slično. Ta lažna stranica šalje posebno pripremljen e-mail koji može izgledati kao npr. obavijest iz banke, u kojem usmjerava korisnike da kliknu na link koji vodi ka lažnoj stranici.

Ukoliko korisnik to uradi, falsifikovana stranica, čiji je izgled gotovo identičan izgledu prave - legitimne stranice, dalje navodi korisnika da upiše svoje lične podatke. Kad korisnik to učini, podaci dolaze do vlasnika lažne stranice, koje on kasnije može zloupotrijebiti.

Lažna web stranica izgleda skoro identična pravoj, ali je URL adresa u traci za adresiranje drugačija, stoga kako biste se zaštitili od pokušaja prevare preporučujemo da kada želite pristupiti stranici Raiffeisen banke, u traku za adresiranje ručno ukucate: raiffeisenbank.ba

Također, naglašavamo da Vam Raiffeisen *BANK* d.d. Bosna i Hercegovina nikada neće poslati e-mail dostavljajući Vam linkove za stranicu na kojoj je potrebno da unesete Vaše korisničko ime, lozinku ili podatke o kreditnoj kartici.

Ukoliko dobijete sumnjiv e-mail, molimo Vas da kontaktirate Banku putem Raiffeisen direkt info telefona: +387 33 75 50 10.

Opšti pojmovi

- **Elementi prepoznavanja** su uređaji koji omogućavaju prijavu korisnika u sistem i autorizaciju plaćanja. Banka izdaje dvije vrste uređaja za identifikaciju:
  - ActivCard čitač + identifikacijska kartica
  - Token
- **Identifikacijska kartica** je sigurnosni mehanizam na kojoj je zapisan digitalni certifikat za svakog korisnika sistema. Digitalni certifikat na kartici je zaštićen osobnom šifrom (PIN).
- **Digitalni certifikat** je skup podataka, koji identificira neki entitet i koji je izdat i digitalno potpisan od strane nekog autoriteta za certificiranje.
- **Čitač kartice** je uređaj koji se priključuje na računar, pomoću kojeg računar komunicira sa identifikacijskom karticom.
- **Token** je uređaj za identifikaciju koji prilikom svakog uključenja dinamički generiše jednokratnu lozinku za prijavu u sistem. Nakon uključenja tokena zahtijeva se unos osobne šifre (PIN).
- **Osobna šifra (PIN)** je kombinacija znakova kojom se štiti pristup do digitalnog certifikata na kartici i dinamičke lozinke na tokenu.

Sigurnost

RBBHnet zadovoljava najrigoroznije sigurnosne standarde i obezbjeđuje visoki nivo sigurnosti transakcija. Također nudi pouzdanu autorizaciju i zaštitu podataka.

Zaštita podataka

Komunikacija između Banke i njenih korisnika se vrši sigurnim kanalom. Da bi se podaci koji se razmjenjuju zaštitili od neovlaštenog čitanja, za njihov prijenos se koristi SSL protokol. Pri tome su svi podaci koje korisnik razmjenjuje sa Raiffeisen *BANK* d.d. Bosna i Hercegovina u svakom trenutku šifrirani upotrebom tog protokola i dijelom korisničkog certifikata zapisanog na odgovarajućem sredstvu identifikacije.

Identifikacija korisnika i autoritzacija plaćanja

Banka svakom ovlaštenom korisniku elektronskog bankarstva izdaje sredstvo identifikacije pomoću kojeg se korisnik prijavljuje u sistem i vrši autorizaciju plaćanja. To su:

- **Kartica sa čitačem**

ili

- **Token**

Prijava u sistem i korištenje aplikacije bez navedenih sredstava identifikacije nije moguća.

Gubitak pametne kartice/tokena:

Korisnik je dužan bez odgađanja prijaviti gubitak/krađu sredstva identifikacije na tel. 033/755 010

Autentičnost Raiffeisen *BANK* d.d. Bosna i Hercegovina na Internetu

Raiffeisen *BANK* d.d. Bosna i Hercegovina posjeduje certifikat izdat od strane svjetski prihvaćenog autoriteta na Internetu, tvrtke VeriSign (http://www.verisign.com). Certifikatom se garantuje autentičnost Raiffeisen banke na Internetu. Zahvaljujući VeriSign certifikatu tokom spajanja na RBBHnet aplikaciju korisnik može biti siguran da zaista komunicira sa Raiffeisen bankom.

Dear Customer,

We wish you a pleasant experience with our Corporate Online Banking Service. Online banking is a high-quality tool that should be used carefully to avoid any difficulties and take advantage of the service's convenience. The security of the system and of our business in general is a basic pillar of our business policy. Continuous improvement of all security aspects is one of our priorities.

The information you exchange with our bank cannot be misused in any way or used for any purpose other than the intended one. All your data is kept and handled in accordance with applicable laws and regulations governing this matter.

Your identification data is your private data and nobody will ever request it from you, nor are you obliged to disclose it to anybody. The same is true for your account or card number.

Customer education is the best, if not the only way to prevent Internet fraud. For the dual purpose of fraud prevention and protection of your data, we would like to make you more sensible against deceptions via email/Internet.

How can you contribute to the security of your business dealings?

- We kindly ask you to pay special attention to the following:
- Keep your identification number, static password and token secret.
- If you have any suspicion that someone might know your personal identification number who is not supposed to, you are obliged to change it immediately. To get instructions how to change your PIN, please
  - contact us by phone at + 387 33 28 78 90, 28 78 91, 28 78 92 or 28 78 93 (Monday - Friday, from 08:30am to 04:30pm) to block the service immediately, or
  - send an e-mail to: : support.desk@rbb-sarajevo.raiffeisen.at.
  - visit our web site on www.raiffeisenbank.ba
- If you have any suspicion that someone might misuse your access to the service, you are required to immediately call our Raiffeisen direct Info + 387 33 75 50 10.
- Close your online banking session by clicking the button "Exit".

We recommend taking the following measures:

- Install an up-to-date anti-virus program version.
- Scan your computer for viruses and spyware once a week.
- Install a private or hardware firewall on your computer.
- Do not share your PIN with anybody.
- Do not conduct online banking from public or insecure computers.
- Do not leave any stickers with your identification data near or on your computer.
- Do not store any documents with your identification data on your computer.
- Do not download any programs from suspicious websites.
- Do not open e-mails with suspicious content.
- Beware of fraudulent e-mails disguised as messages from Raiffeisen Bank.

A very frequent variation of deception is ***phishing***. It is aimed at worming out secret data from Internet users, such as user names, passwords and card data, for fraudulent use.

Phishing is done via faked websites disguised, for example, as online payment sites, a bank or a popular social network site etc. That fake website sends a specially created e-mail which can look like a notice from a bank, luring users to click on a link that guides them to a faked website.

Once connected to these deceptive imitations, users are asked to enter secret personal data. If they follow the instruction, their data will be transmitted to the owner of the faked website, who can use them fraudulently at a later time.

The fake website is almost identical to the true one, but the URL address in the address line is different. We therefore recommend you, in order to protect yourself from fraud, to access Raiffeisen Bank's website by manually entering its address raiffeisenbank.ba into the address line.

Also note, that Raiffeisen *BANK* d.d. Bosna i Hercegovina will never send you an e-mail asking you to connect to websites where you will be asked to enter your user name, password or credit card data.

If you get a suspicious e-mail, please call the Raiffeisen direct info line: +387 33 75 50 10.

Definitions

- **Recognition elements** are devices that enable the user to log into the system and authorise payments The bank issues two types of identification devices:
  - ActivCard reader + card identification
  - Token
- **Identification card** is a security mechanism that includes a recorded digital certificate for each user of the system. The digital certification the card is protected

Security

RBBHnet satisfies the most rigorous safety standards and provides high level of transaction security. It is also offering a reliable authorisation and data protection.

Data protection

Communication between the Bank and its users is conducted through safe channel. In order to protect data exchanged from unauthorised reading SSL protocol is used for their transfer. In doing this all data exchanged between user and Raiffeisen *BANK* d.d. Bosnia & Herzegovina are at any time coded by using the above protocol and partially user's certificate encrypted on a respective mean of identification.

User Identification and Payment Authorisation

The Bank issues to any autorised electronic banking user a mean of identification by which a user is accessing the system and makes payment authorisation. These are:

- **Card reader**


or

- **Token**

Access to system and using application without the above means of identification is not possible.

Loss of Smart Card/Token:

A user is obliged without any delay to report the loss/stealing of identification means on phone no. 033/755-010

Authenticity of Raiffeisen *BANK* d.d. Bosnia & Herzegovina on Internet

Raiffeisen *BANK* d.d. Bosnia & Herzegovina owns a certificate issued by world-accepted authority on Internet, the company VerSign (http://www.verisign.com).
This certificate is guaranteeing Raiffeisen bank authenticity on Internet. Due to VeriSign certificate a user may be secure that he/she is really communicating with Raiffeisen bank during his/her connection to RBBHnet application.