Važne informacije o bezbednosti Vaših informacija

Adriatic Bank a.d. Beograd je opredeljena da zaštiti Vaše lične podatke kao i finansijske transakcije i novac. Ostvarujemo naš cilj kombinovanjem programa za prevenciju prevare, analitičkih alata i pozadinskih procesa s ciljem analize i preciznog određivanja sumnjivih radnji. Opisani postupci nam pomažu da sprečimo prevaru i uverimo Vas da su Vaši lični podaci, podaci o finansijama, kao i Vaš novac bezbedni kroz sve kanale kojima pružamo bankarske usluge (putem Interneta, kroz mrežu filijala i putem telefonskih poziva). Internet je postao pogodno mesto za kriminalce da dođu do raznih informacija od Vašeg bankarskog računa do ličnih podataka. Dobra strana je što postoje jednostavni načini da zaštitite svoje Internet račune kao i kompjutere.

Bezbednost transakcija na Internetu i elektronske pošte

• Uvek pristupajte našim elektronskim bankarskim servisima (Adriatic Bank eBank) kroz zvaniči sajt Adriatic Bank na web adresi **www.** adriaticbank.rs
• Nikada ne treba da verujete ili pružate informacije o Vašem korisničkom nalogu na web stranama koje koriste ime Adriatic Bank kojima niste pristupili kroz zvaničan sajt banke.
• Nikome nemojte davati podatke o Vašem korisničkom nalogu za elektronske bankarske servise (elektronsko bankarstvo i trgovina).
• Zaposleni Adriatic Bank a.d. Beograd nikada neće tražiti da kažete Vaš PIN ni preko telefona ni putem email poruke ili na ma koji drugi način.
• Ne pristupajte svom bankarskom računu ili ma kom drugom finansijskom servisu iz Internet kafea ili drugih javnih mesta.
• Ograničite finansijske informacije na Vašem laptop-u i mobilnim uređajima.
• Nikada ne napuštajte kompjuter u toku korišćenja elektronskih bankarskih usluga (elektronsko bankarstvo i trgovina).
• Ne odgovarajte na email poruke koje imaju izgled i sadržaj kao da su od Adriatic Bank državne institucije ili ma kog drugog tela a koje zahtevaju da dostavite lične podatke u smislu korisničkog imena, lozinke, PINa i sl.
• Obrišite poruke tipa *spam* ili koje sadrže sumnjive priloge.
• Nemojte otvarati neočekivane priloge bez obzira da li dolaze od poznatog ili nepoznatog korisnika.
• Podesite primanje SMS obaveštenja o stanju na računu i obavljenim finansijskim transakcijama s računa direktno ili putem elektronske kartice kao vid sigurnosnog mehanizma praćenja finansija.
• Povremeno će Adriatic Bank putem elektronske pošte slati obaveštenja o marketinškim kampanjama. Gde je to moguće koristićemo Vaše ime s ciljem potvrde da je naša komunikacija pouzdana. Nećemo tražiti da otkrijete lične ili bezbednosne informacije putem elektronske pošte i nikada Vas nećemo direktno preusmeravati na stranu koja služi za logovanje na elektronsko bankarstvo ili drugu sličnu aplikaciju.
• Ukoliko primite email koji traži da 'verifikujete svoj nalog', 'potvrdite detalje u vezi sa logovanjem' ili slično sročen zahtev, možete biti sigurni da je u pitanju prevara na koju ne treba reagovati.

Zaštita od virusa, Spyware i Firewalls

• Obavezno instalirajte antivirusni program.
• Koristite mehanizme detekcije malicioznih softvera poput spyware, malware, spam-a kao i programe za njihovu eliminaciju.
• Koristite softvere zaštite (*firewall* ili *personal firewall*), posebno ukoliko imate konekciju viskog propusta ili stalni pristup Internetu poput DSL ili kablovskog modema.
• Proverite da li se definicije virusa kao i anti-spyware redovno ažuriraju.
• Radite redovna i česta skeniranja kompjutera kako biste otkrili viruse ili slične nepoželjne i maliciozne softvere (poput *spyware*-a i *malware*-a).
• Ažurirajte svoje operativne sisteme i softvere instaliranjem najnovijih softverskih 'zakrpa' (eng. Security patches) tj. dodataka na postojeće verzije kojima se unapredjuje ili poboljšava rad i sigurnost postojeće verzije softvera.

Bezbednost korisničkog pristupa i zaštita PIN koda

• Nikada nikome ne pokazujte svoj PIN kod.
• Kada se logujete na našu aplikaciju elektronskog bankarstva (eBanking), proverite da li Vas neko posmatra.
• Izbegavajte da koristite automatsko logovanje koje pamti PIN kod.
• Uvek uradite izlaz iz internet servisa regularnim mehanizmom koju aplikacija predviđa, nikada nemojte samo da zatvorite aplikaciju ili brauzer.
• Omogućite opciju kojom se kompjuter zaključava posle određenog vremenskog perioda neaktivnosti ("time out" opcija).
• Nikada ne zapisujte PIN kod gde bi drugi mogli da ga pročitaju.
• Kada birate lozinku, nemojte koristiti informacije koje se mogu lako povezati s Vama kao što su datum rodjenja, broj pasoša, matični broj i slično.
• Vršite izmenu lozinke često s ciljem povećanja bezbednosti preporučujemo jednom mesečno.
• Izbegavajte da koristite iste ili prethodno korišćene lozinke.

Bezbednosni uređaji - tokeni (Security Tokens)

• Uvek nosite sa sobom tokene.
• Nikome ne otkrivajte jednokratno dodeljene PIN kodove (One Time Pin kodove) koji su vezani za token.
• Zaposleni Adriatic Bank vam nikada neće tražiti da otkrijete jednokratno dodeljeni PIN kod (OTP) preko telefona (ili na neki drugi način)
• Izbegavajte izlaganje tokena ekstremno visokim ili niskim temperaturama na duži period. Tokeni nisu otporni na vodu.

Bezbednosni saveti za korisnike- pravna lica koji imaju račun u našoj banci

• Odredite gornji dnevni limit za novčane transakcije za svaki od računa kompanije koji ste otvorili po raznim osnovama.
• Primenite mehanizme višestrukog potpisa. Na ovaj način definišete nivoe ovlašćenja za potpisivanje. Dakle, transakcije kreirane od strane jednog zaposlenog bice automatski usmerene na dodatnu potvrdu od strane drugog nadležnog pre nego što se izvrše.
• U slučaju *prestanka radnog odnosa zaposlenog* u Vašoj kompaniji koji je do tada bio

korisnik ili ovlašćeni korisnik, uradite sledeće:
• Obavestite Adriatic Bank tako da se onemogući pristup sistemu.
• Nemojte po automatizmu preneti iste korinsičke kodove za pristup niti digitalne potpise novom zaposlenom.
• Uništite sve kompjuterske fajlove koji sadrže kopije digitalnog sertifikata koji je bio u upotrebi od strane bivšeg zaposlenog.
• Podnesite zahtev za novi sertifikat.

Bezbednosne preporuke - šta činiti i šta ne činiti

• Ne preuzimajte datoteke od nepoznatih lica i sa nepoznatih sajtova.
• Ne klikćite na link u email porukama koje primite od nepoznatog pošiljaoca.
• Koristite usluge elektronskog bankarstva – time obezbeđujete elektronsku evidenciju bankarskih transakcija i smanjujete papirologiju, istovremeno imate mogućnost redovnog uvida u svoje bankarske izvode.
• Obrišite sve lične informacije koje se nalaze u vašem kompjuteru pre nego što se odlučite na njegovu prodaju ili ga ustupite na korišćenje drugoj osobi. Postoje takozvani "wipe" alati koji pišu preko postojećeg i na taj način pouzdano brišu sadržaj na disku.
• Preporučujemo da pročitate politike o privatnosti na Web sajtu koji posetite za sva pitanja i odgovore u vezi pristupa, tačnosti, bezbednosti i kontrole ličnih podatka koje sajt prikuplja, a takođe i koliko će osetljive podatke sajt da koristi i da li će biti ustupljeni trećim stranama.
• Wireless opremu instalirajte pravilno. Čitajte instrukcije i pratite preporuke proizvođača u vezi sa primenom sigurnosnih mehanizama i konfiguracije.

'Phishing' elektronske poruke – korisne informacije

• Ukoliko primite elektronsku poštu koja izgleda kao da je poslata od strane Adriatic Bank a.d Beograd koja traži da ukucate svoj korisnički nalog i šifru, nemojte to učiniti: verovatno se radi o prevarantima koji pokušavaju da ukradu vaš novac.
• Osobe odgovorne za slanje prevarantskih poruka vas ne poznaju lično već šalju tipične poruke na hiljade elektronskih adresa do kojih dođu. Cilj poruke je upravo da dođu do ličnih informacija.
• Po pravilu link koji se nalazi u poruci preusmeriće vas na internet sajt koji traži izmenu ili verifikaciju podataka. Takve poruke i sajtovi mogu delovati uverljivo pa je najsigurniji način zaštite da ne kliknete na ponuđeni link ili ako ste to već uradili, da ne odgovarate na pitanja o detaljima pristupa.
• Dešavaće se da ove strane liče na strane Adriatic Bank a.d. Beograd ili elektronske bankarske aplikacije, ali nikada nemojte da kliknete na link u elektronskoj poruci koja imitira stranu prema aplikaciji elektronskog bankarstva. Ukoliko ste u ma kom trenutku u nedoumici oko autentičnosti internet strane, setite se da proverite sertifikat strane. Ukoliko primite elektronsku poštu za koju sumnjate da je u pitanju prevara ne odgovarajte i ne dajte informacije. Obavestite nas slanjem elektronske poruke na adresu kartice@adriaticbank.rs sa naznakom u polju Subject: – Ugrožena bezbednost informacija
• Ukoliko ste ipak odgovorili na poruku gde je u pitanju prevara i dali lične podatke, kontaktirajte naš korisnički centar putem telefona 0800 330 300 ili 011 33 06 300 (pozivi su besplatni sa mreže fiksne telefonije).

• Ukoliko korisnički centar nije u funkciji morate uraditi sledeće:
• ODMAH promenite svoj PIN i lozinku.
• Ukoliko su prevaranti već promenili detalje Vašeg naloga i ne uspete da se ulogujete, uradite više uzastopnih pokušaja koji će biti neuspešni ali će prouzrokovati zaključavanje naloga i time inicirati povlačenje prijave.
• Proverite bankarski izvod računa s ciljem pronalaženja sumnjivih transakcija koje treba da pribeležite i izvestite banku o pokretanju istrage.
• Kontaktirajte korisnički centar sledećeg radnog dana.