Osnovne preporuke za bezbednu upotrebu RaiffeisenOnLine elektronskog bankarstva

Poštovani klijenti,

Dokument navodi osnovne preporuke vezane za bezbednu upotrebu RaiffeisenOnLine. Neophodno je da se korisnici pridržavaju ovih uputstava kako bi adekvatno zaštitili uređaje na kojima koriste elektronsko bankarstvo.

Posebna pažnja posvećena je zaštiti i pravilnoj upotrebi podataka i informacija koje su neophodne za korišćenje RaiffeisenOnLine, kao što su kartica/USB sa sertifikatom, PIN i drugi.

Obratite pažnju na sledeće:

Prevare koje se obavljaju putem telefonskih poziva

Popularan način prevara je pozivanje klijenata putem telefona, pri čemu se zlonamerni akteri lažno predstavljaju kao službenici banke i pokušavaju da saznaju Vaše lične podatke (JMBG, PIN, broj mobilnog telefona, podatke za aktivaciju i pristup elektronskom bankarstvu i slično) ili podatke o firmi.
Često se pritom upravo pozivaju na bezbednosne provere prividno u ime banke, kako ne bi pobudili sumnju kod korisnika.
Nikada nemojte saopštavati svoje lične podatke na osnovu ovakvih zahteva, čak i ako se od Vas traži da „zbog sigurnosnih razloga" pozovete službenika banke na određeni telefon koji Vam je ponuđen.
Kontakt sa bankom putem telefona, isključivo obavljajte putem kontakt centra Banke i broja telefona objavljenog na zvaničnoj internet stranici banke.

PIN

PIN tretirajte kao lični podatak i nikada ga ne saopštavajte drugim licima. Izričita je preporuka da PIN *nikada* ne zapisujte bilo gde, i svakako da ga ne čuvate u blizini kartice/USB sa sertifikatom.
Molimo Vas da se prema kartici/USB sa sertifikatom i PIN-u odnosite odgovorno, na isti način kao što se odnosite prema Vašim ličnim dokumentima (na primer platnoj kartici).

Nikada ne ostavljajte karticu/USB sa sertifikatom u čitaču kartica kada je ne koristite. Kada ne koristite karticu/USB, čuvajte ihe na adekvatno obezbeđenom mestu.

Kartica/USB i PIN se dodeljuju lično, personalizovano za određenog korisnika. U cilju bezbednog korišćenja RaiffeisenOnLine aplikacije u Vašoj firmi, Vašu karticu/USB i PIN nemojte deliti sa drugim kolegama.

Fišing (engl. *phishing*)

Fišing je veoma rasprostranjen način prevare. Kradljivci identiteta se predstavljaju, najčešće putem imejl poruka, kao finansijske ustanove, kompanije ili kao banka. Zlonamernim porukama, pokušava prevaranti Vas naveode da otkrijete lične podatke, podatke za pristup RaiffeisenOnLine ili aktivaciju i upotrebu mobilne aplikacije. Nemojte odgovarati na ovakve poruke i ne posećujte linkove koji su navedeni u samim imejl porukama.

Raiffeisen banka Vam nikada neće slati imejl poruke u kojima se zahteva da saopštite Vaš PIN ili druge lične podatke. Banka nikada ne koristi imejl za pribavljanje ličnih ili poverljivih informacija od klijenata. Takođe, Raiffeisen banka Vam nikada neće slati imejl poruke u kojima od Vas traži da pozovete kontakt centar banke na broj telefona koji se nalazi u poruci i ostavite Vaše lične podatke

Upotreba elektronskog bankarstva sa tuđih uređaja

Kada koristite online bankarstvo, uverite se da Vam niko ne vidi korisničko ime, lozinku ili PIN dok koristite RaiffeisenOnLine.

Ukoliko ne radite sa svog uređaja, imajte na umu da uređaj može biti kompromitovan ili zaražen zlonamernim softverom. Preporučujemo da nakon korišćenja RaiffeisenOnLine sa tuđih uređaja promenite Vaš PIN kada budete u prilici da to uradite sa bezbednog uređaja. Preporuka je da ne pristupate RaiffeisenOnLine sa javnih uređaja, kad god je to moguće izbeći.

Prijava bezbednosnih incidenata

Ukoliko smatrate da ste bili žrtva napada koji su ranije pomenuti ili imate bilo kakve dileme vezano za imejl ili SMS poruke u kojima se pominje Raiffeisen banka molimo Vas da nas kontaktirajte na tel. **+381 (0)11 3202 100** ili pošaljite poruku na adresu abuse@raiffeisenbank.rs.

Kako zaštititi uređaj koji koristite

Sledeće preporuke namenjene su prvenstveno za firme koje nemaju specijalizovanu službu ili lice nadležno za informacioni sistem.

Antivirusni programi

Neophodno je da na Vašem uređaju postoji instaliran antivirusni program (listu pouzdanih i afirmisanih proizvođača možete naći na sledećem linku: https://support.microsoft.com/en-US/windows-antivirus-software-providers). Efikasnost u otkrivanju zlonamernog softvera direktno zavisi od toga da li se program redovno ažurira antivirusnim definicijama. Preporuka je da se proces ažuriranja antivirusnog softvera obavlja automatski.

Obratite pažnju: na Internetu se mogu naći prividno besplatni antivirus programi koji su razvijeni od strane kriminalaca i najčešće u sebi sadrže zlonamerne programe. Korišćenje proverenog i renomiranog antivirusnog rešenja je neophodan preduslov za pouzdanu zaštitu.

Programi za mrežnu zaštitu *(*engl. *Personal Firewall)*

Preporučujemo da na svom uređaju instalirate ili aktivirate program za mrežnu zaštitu i time umanjite mogućnost neovlašćenog pristupa Vašem uređaju od strane nepoznatih lica. Operativni sistemi Microsoft Windows imaju već ugradjen firewall program koji je je neophodno aktivirati/uključiti.
Preporuka je da na uređaju (serveru ili ruteru) pomoću koga Vaša firma pristupa Internetu postoji instaliran firewall podešen da minimizuje dozvoljenu komunikaciju samo na neophodne servise.

Redovno instaliranje ispravki i dopuna (engl. *installing of patches and updates*)

Proizvođači softvera periodično objavljuju ispravke i dopune za operativne sisteme i aplikacije, u cilju otklanjanja sigurnosnih ili funkcionalnih nedostataka i neophodno ih je redovno instalirati. Windows i drugi programi mogu da ovu funkciju obavljaju automatski; proverite da li je ova opcija uključena.
Važno: koristite isključivo dopune i ispravke koje su objavljene na zvaničnim stranicama proizvođača. Hakeri šalju imejl poruke ili Vas putem pop-up prozora navode da instalirate lažne dopune i ispravke koje sadrže zlonamerne programe, pri čemu se često kao razlog navode upravo bezbednosni propusti i zahteva hitno reagovanje.

Upotreba legalnih programa

Preporuka je da koristite isključivo legalno nabavljen softver i operativne sisteme. Nelicencirane ili kopije su često zaražene zlonamernim programima (na primer raznim vrstama virusa ili trojanaca).

Upotreba Web pregledača (engl. *Web browsers*)
Za pristupanje RaiffeisenOnLine koristite preporučene verzije Web pregledača iz dokumenta Pravila i uslovi za korišćenje usluga RaiffeisenOnLine elektronskog bankarstva. Aktivirajte opciju Anti phishing filtriranja ukoliko je dostupna.

Pre nego što se ulogujete na RaiffeisenOnLine, bezbednost Vaše sesije možete proveriti u pregledaču na način sličan prikazanom na slici niže (na slici je primer za Microsoft Edge).

Ukoliko bilo koje polje sadrži drugačije podatke od onih prikazanih na slici, nemojte počinjati sa radom i obavezno pozovite kontakt centar Banke na tel: +381 (0)11 3202 100