UNIONBANKA
Union Banka dd Sarajevo
Dubrovačka br. 6, 71000 Sarajevo
+387 33 561 000
+387 33 219-201
info@unionbank.ba
www.unionbank.ba

Savjeti klijentima za sprečavanje zloupotreba prilikom korištenja UNIONNET elektronskog bankarstva

Sigurnost i primjena opšteprihvaćenih sigurnosnih rješenja predstavljaju osnovu UNIONNET elektronskog bankarstva. Komunikacija između web pretraživača korisnika elektronskog bankarstva i servera odvija se preko tzv. SSL (secure socet layer) protokola, što omogućava šifrovan prenos podataka i autoidentifikaciju korisnika i servera. SSL protokol predstavlja siguran način prenosa povjerljivih podataka preko interneta i obzirom da se radi o kriptovanom prenosu, onemogućeno je presretanje ili mijenjanje poruka.

Banka sa svoje strane čini sve kako bi se klijenti zaštitili, unaprjeđujući kontinuirano sve sigurnosne mjere, međutim, najvažnije je da korisnici elektronskog bankarstva budu svjesni potencijalnih opasnosti i da se pridržavaju preporuka o sigurnosti na internetu. Edukacija korisnika predstavlja svakako jedan od osnovnih načina sprečavanja prevara i nezakonitih radnji putem interneta.

Šta je to ”phishing”?

”Phishing” ili ”pecanje” podataka, predstavlja pokušaj krađe podataka poput korisničkih imena,lozinki ili podataka s platnih kartica s ciljem zloupotrebe istih i ostvarivanja protupravne materijalne koristi. Phishing se uglavnom izvodi putem lažnih elektronskih poruka u kojima se od korisnika traži da pokrene priloženi fajl, čiji je sadržaj obično maliciozan ili da slijedi poveznice (linkove) u poruci i na taj način pošiljaocu otkrije povjerljive informacije.

Ukoliko slijedi linkove u lažnoj poruci, korisnik će biti preusmjeren na lažnu, falsifikovanu web stranicu (npr. stranica za on line plaćanje, društvena web stranica i sl.) čiji je izgled obično identičan originalnoj, pravoj stranici i gdje se korisnik navodi da unese svoje lične podatke. Na taj način, svi podaci koje korisnik unese, vidljivi su i prevarantima koji su inicijalno i kreirali „phishing“ elektronsku poruku sa ciljem krađe novca sa bankovnog računa ili zloupotrebe podataka.

Lažna web stranica je vizuelno identična originalnoj ali je URL adresa drugačija. S tim u vezi, kada želite pristupiti stranici Union banke, preporuka je da u prostor za adresiranje ručno unesete web adresu Union banke: www.unionbank.ba

Kako se zaštititi?

Union banka nikada neće tražiti vaše lične podatke kao što su korisničko ime, lozinka, pin kod, broj platne kartice, CVV broj i sl. Union banka nikada ne dostavlja komitentima elektronske poruke gdje se traži otkrivanje navedenih podataka ili slijeđenje linkova. Lični podaci su namijenjeni i poznati isključivo vama i niko nema pravo od vas tražiti ove podatke, stoga vodite strogo računa o vašim ličnim podacima. Otkrivanjem ličnih podataka izlažete se visokom riziku prevare, materijalnog gubitka, zloupotrebe podataka i potencijalnoj krađi identiteta.

od 1955

Nikada nemojte slijediti linkove niti otvarati priloge (attachment) iz elektronskih poruka koje ste dobili od nepoznatog pošiljaoca. Budite posebno oprezni pri otvaranju poruka koje Vam navodno šalje banka a znate da niste poslali izričit zahtjev za slanje poruka. Nemojte otvarati linkove iz tzv. „pop-up prozora“, u ovakvim prozorima se ne nalazi ispravna adresa elektronskog bankarstva. Ograničite količinu ličnih podataka javno dostupnih na internetu.

Union banka će vam dostavljati informacije o svim eventualnim promjenama (nadogradnja, nova verzija i sl.) isključivo u okviru interfejsa UNIONNET-a. Pojednostavljeno, obavještenja možete preuzeti i čitati isključivo tek kada se uspješno prijavite na stranicu elektronskog bankarstva, koristeći validne podatke za identifikaciju.

Pri svakom pristupanju uvijek pažljivo pregledajte web adresu banke (www.unionbank.ba) U odnosu na autentičnu web adresu banke, adresa lažne ili podmetnute stranice od strane napadača može imati samo jedno slovo, znak ili tačku razlike i na prvi pogled može izgledati identično. Nakon što otvorite prozor gdje ćete unijeti vaše kredencijale za pristup UNIONNET-u, provjerite da stranica koristi zaštićeni sigurnosni protokol, (SSL) te valjanost digitalnog certifikata. Provjerite da li web adresa počinje sa https:// što ukazuje na korištenje kriptovanog kanala komunikacije. Mali katanac koji se obično nalazi u desnom donjem uglu Vašeg preglednika ili u desnom dijelu polja u koji unosite web adresu stranice, ovisno koji web pretraživač se koristi, potvrđuje da je web adresa banke potpisana ispravnim certifikatom (*Verfied by: VeriSign, Inc.)*

Za dodatnu provjeru identiteta koristi se miniToken. MiniToken je sigurnosni uređaj koji se koristi za identifikaciju korisnika prilikom prijave u sistem UNIONNET-a. Identifikacija korisnika se vrši na osnovu 3 elementa (fizička lica):

- Jednokratne, promjenjive dinamičke lozinke koju generiše miniToken. Nakon svakog generisanja lozinke, vrijednost dinamičke lozinke je različita od svih prethodnih, a buduću vrijednost nije moguće predvidjeti.
- Korisničkog imena, koje je jedinstveno za svakog korisnika UNIONNET-a i dodjeljuje ga administrator Banke.
- Statičke lozinke koja je jedinstvena za svakog korisnka, minimalno 8 karaktera, a samo prvi put se dodjeljuje od strane administratora banke.

Pravna lica pristupaju koristeći dinamičku lozinku koju generiše token i korisničko ime.

Obavezno koristite pouzdan antivirus program i koristite isključivo licenciran i ažuran operativni sistem, kao i legalnu računarsku opremu. Uvijek koristite najnoviju verziju web pretraživača, što uključuje i redovno ažuriranje sigurnosnih postavki. Uključite vatrozid (firewall) unutar operativnog sistema. Ne koristite nepotrebne dodatne web pretraživače i ne preuzimajte dodatke sa neprovjerenih i sumnjivih lokacija. Ne posjećujte stranice sumnjivog karaktera, stranice ilegalnog softvera, sumnjivih poslovnih ponuda i sl.

Koristite tzv. „jake lozinke“ koje sadrže kombinaciju slova, brojeva, posebnih znakova, znakova interpunkcije i sl, minimalne dužine 8 znakova. Vaša lozinka je samo Vaša i nemojte je dijeliti sa drugima. Uvijek se odjavite (log off) kada privremeno odlazite od računara, kako bi se izbjegao neovlašteni pristup.

Izbjegavajte korištenje medija i USB memorijskih uređaja nepoznatog porijekla, vanjski mediji predstavljaju čest izvor zaraze malicioznim kodom.

od 1955

Veoma je bitno pridržavati se dosljedno svih navedenih preporuka kako bi se zaštitili od napadača i kako bi se spriječila eventualna kompromitacija i zloupotreba Vaših podataka.

Sta raditi u slučaju zloupotrebe?

Ukoliko sumnjate da bi neko mogao zloupotrijebiti Vaš pristup servisu ili ukoliko sumnjate da neko posjeduje vaše kredencijale za pristup elektronskom bankarstvu ili ukoliko želite prijaviti krađu ili gubitak token-a, ili ukoliko imate bilo kakve dodatne nedoumice ili sumnje, informacije možete dobiti:

- Putem telefona: ++387 33 561 062; 561 074
- Putem elektronske pošte: unionnet@unionbank.ba

od 1955