Informacije o internet bezbednosti: „Fišing“ ili mrežna krađa identiteta

Šta je „fišing“?

„Fišing“ ili mrežna krađa identiteta predstavlja pokušaj krađe podataka korisnika interneta putem falsifikovane *web* stranice. Obično se link za takvu stranicu nalazi u *e-mail*-u ili *chat* porukama koje se nasumično šalju, u pokušaju da se klijenti prevare i navedu da otkriju informacije na lažnoj *web* stranici.

U tim porukama obično se tvrdi da je neophodno „ažurirati“ ili „potvrditi“ informacije o vašem računu, te se klijenti nagovaraju da kliknu na dati link u elektronskoj poruci/*e-mail*-u koja ih vodi do lažne *web* stranice. Sve informacije koje upišete na lažnoj *web* stranici dospevaju u ruke kriminalaca koje oni zatim koriste u svoje nezakonite svrhe.

Kako izbeći da postanem žrtva fišinga?

Najvažnije je da imate određenu dozu sumnje prema svim neželjenim ili neočekivanim elektronskim porukama koje primite, čak i kada se čini da potiču iz poverljivog izvora.

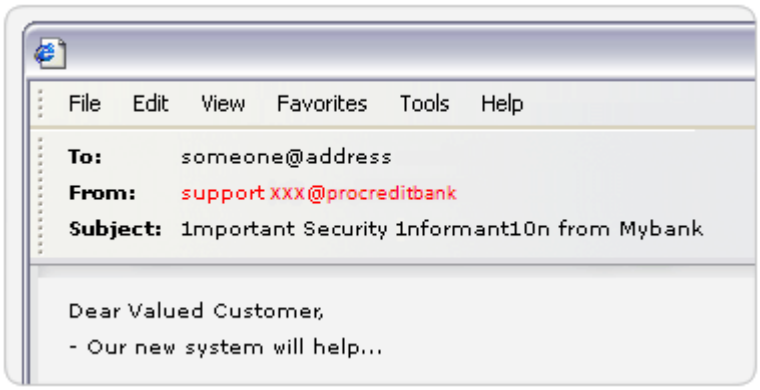
Te poruke se šalju potpuno nasumično u nadi da će stići na aktivnu elektronsku adresu klijenta sa računom u ciljanoj banci.

Iako vam se ProCredit banka može obratiti putem elektronske poruke, ProCredit banka vam nikad neće poslati poruku kojom od vas zahteva da upišete svoju lozinku ili bilo koje druge poverljive podatke tako što ćete klikom na *link* posetiti neku *web* stranicu.

Sačekajte malo i razmislite kako vaša banka inače komunicira sa vama i nikada nemojte otkrivati svoju punu lozinku ili bilo koje lične podatke.

Kako prepoznati fišing elektronsku poruku?

1 – Od koga je elektronska poruka?



„Fišing“ poruke mogu izgledati kao da dolaze sa prave elektronske adrese ProCredit banke. Nažalost, zbog sistema elektronskih poruka, licima koja se bave ovim nezakonitim radnjama je relativno jednostavno da kreiraju lažni upis u polju „Od“ (From).

Adresa elektronske pošte koja se pojavljuje u polju „Od“ u poruci NIJE garancija da dolazi od lica ili organizacije navedene u adresi elektronske pošte. Ove poruke nisu poslate preko sistema banaka.

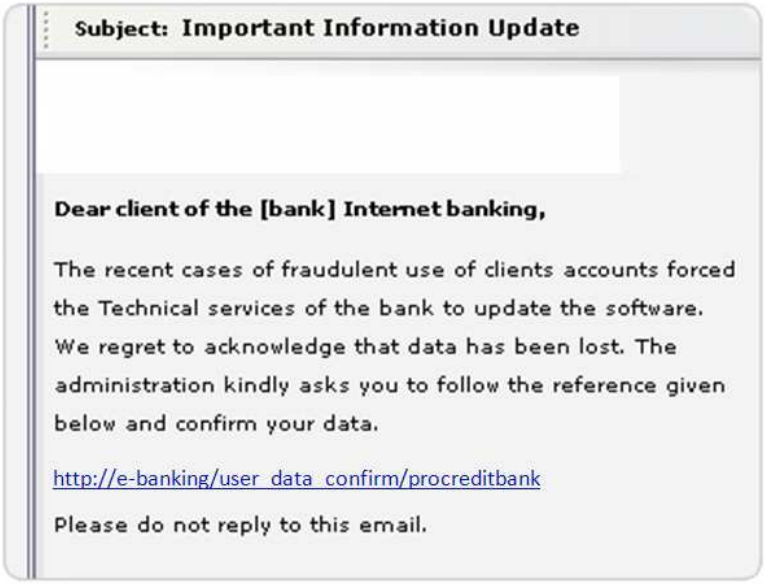
2 – Za koga je elektronska poruka?

Elektronske poruke se šalju nasumično na veliki broj adresa i lica koja se time bave gotovo sigurno ne znaju vaše pravo ime, niti bilo šta drugo o vama, te vas oslovljavaju uopštenim izrazima poput „Poštovani, cenjeni klijente“.

3 – Pogledajte pažljivije elektronsku poruku – da li izgleda sumnjiva?

Prva stvar koju je važno zapamtiti jeste da vam banke nikada neće pisati i od vas tražiti lozinku ili druge poverljive podatke putem elektronske poruke.

Isto tako, poruka najverovatnije sadrži neobično napisane reči ili neobično upotrebljena velika i mala slova u polju „Predmet“ (Subject): (ovo je pokušaj da se zaobiđe filter programa koji čisti spam), kao i gramatičke i ortografske greške.



Jedan od primera „fišing“ elektronske poruke

Nikada se ne prijavljujte na svoj nalog za elektronsko bankarstvo klikom na link koji je dat u elektronskoj poruci/*e-mail*-u.

Naša preporuka je da koristite linkove koji se nalaze na zvaničnom *web site*-u ProCredit banke (***www.procreditbank.rs***) ili u *adress bar browser*-a sami unesite internet adresu ProCredit banke za elektronsko bankarstvo.

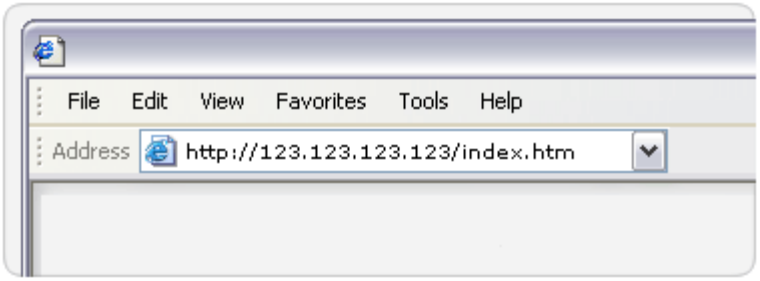
Ako imate bilo kakve nedoumice u vezi sa validnošću elektronske poruke koja navodno predstavlja ProCredit banku, sumnjivu poruku možete proslediti na sledeću adresu elektronske pošte ***ebankar@procreditbank.rs***. Takođe Banci se možete obratiti telefonskim putem, pozivom našeg Info centra na broj telefona **0 700 700 000** ili **011/20 57 000** (za pozive sa mobilnog telefona i iz inostranstva) ili tako što ćete posetiti najbližu ekspozituru i uspostaviti kontakt sa vašim savetnikom za klijente.

4 – Kuda vodi hiperlink?

Nažalost, previše je jednostavno zamaskirati pravu destinaciju *link*-a, tako da se prikazani link može lako falsifikovati, kao i sve što se pojavljuje u statusnoj traci (status bar-u) vašeg programa za elektronske poruke.

Kako prepoznati fišing internet stranicu?

Koja je adresa internet stranice?



Ako posećujete *web* stranicu klikom na link dat u elektronskoj poruci/*e-mail*-u, postoji mnogo načina da se zamaskira prava lokacija lažne *web* stranice u traci sa adresom (address bar-u). Adresa stranice može počinjati nazivom domena prave stranice, ali nema garancije da ona i vodi do prave stranice.

Među drugim trikovima se nalazi korišćenje numeričkih adresa, registrovanje sličnih adresa (kao što je **www.mybank-verify.com**) i čak umetanje lažne trake sa adresom (lažnog address bar-a) u prozor *web browser*-a. Mnogi linkovi sa tih stranica mogu zaista i voditi do prave internet stranice, ali ne dopustite da vas to zavara.

Možete proveriti da li se nalazite na službenoj, bezbednoj *web* stranici ProCredit banke upoređivanjem simbola za bezbednu vezu (kao što je prikazano na slici).

Kliknite na ikonu „katanca“ i videćete uverenje o bezbednosnoj identifikaciji web stranice.

Možete proveriti **Security Certificate (uverenje o bezbednosti)** internet stranice ProCredit banke klikom na „katanac“ koji se pojavljuje na vašem *web browser*-u.

Čuvajte se falsifikovanih pojavnih (pop-up) prozora

Umesto da prikažu u potpunosti lažnu *web* stranicu, lica koja se bave „fišingom“ mogu učitati autentičnu *web* stranicu u prozor glavnog *web browser*-a, a zatim staviti svoj vlastiti lažni pojavni prozor koji će se pojavljivati preko nje.

Ako je stranica prikazana na ovaj način, videćete traku sa adresom (*address bar*) autentične *web* stranice u pozadini, ali će sve podatke koje upišete u pojavnom prozoru pokupiti prevaranti za svoju vlastitu upotrebu.

Kako biste pristupili nalogu za elektronsko bankarstvo, sami upišite adresu u novom prozoru ili koristite linkove koji se nalaze na zvaničnom *web site*-u ProCredit banke (***www.procreditbank.rs***). Adresa vaše autentične stranice za elektronsko bankarstvo počinje sa „https“ i sadrži mali katanac na prozoru *web browser*-a.