ProCredit Bank

e-Banking

Bezbednosne informacije na mreži

ProCredit Bank je posvećena zaštiti integriteta vaših transakcija i podataka o bankovnom računu. ProCredit Bank stoga koristi najnoviji sigurnosni softver i procedure za zaštitu vaših online transakcija. Ipak, uvek morate biti svesni da se Internet i e-pošta mogu koristiti kao sredstva za ilegalne aktivnosti, pa vam preporučujemo da preduzmete neke jednostavne mere opreza kako biste osigurali bezbednost.

Saveti za bezbednost na mreži

Znajte sa kim imate posla
Uvek pristupite Internet bankarstvu tako što ćete uneti adresu banke u svoj veb pregledač [https://ebanking.procreditbank-kos.com]. Nikada nemojte da idete na veb lokaciju sa nekog linka u e-pošti i da tu unesete lične podatke. Ako ste u nedoumici, kontaktirajte ProCredit Bank na: [+383-38 / 555-555 ili +383-49 / 555-555].

Čuvajte lozinke i PIN -ove na sigurnom
Uvek budite oprezni u vezi sa neželjenim e -porukama ili pozivima koji traže od vas da otkrijete lične podatke ili brojeve kartica. Čuvajte ove podatke u tajnosti. Budite oprezni u otkrivanju ličnih podataka nekome koga ne poznajete. Vaša banka i policija vas nikada neće kontaktirati i tražiti da otkrijete svoje PIN -ove ili podatke o lozinki.

Držite se vaše gotovine!
Neka vas ne zavaravaju e-poruke koje iskreno izgledaju a koje vam nude priliku da lako zaradite. Ako izgleda previše dobro da bi bilo istinito, verovatno jeste! Budite posebno oprezni u vezi sa neželjenim e-porukama izvan zemlje - biće mnogo teže proveriti da li su to oni za koje kažu da jesu.

Neka vaš računar bude siguran
Koristite najnoviji antivirusni softver i lični zaštitni zid i, ako vaš računar koristi operativni sistem Microsoft Windows ažurirajte ga putem Microsoft veb lokacije. Uvek koristite najnoviju verziju svog Internet pregledača koja uključuje sva bezbednosna ažuriranja. Budite posebno oprezni ako koristite internet kafiće, biblioteke ili bilo koji drugi računar koji nije vaš i nad kojim nemate kontrolu.

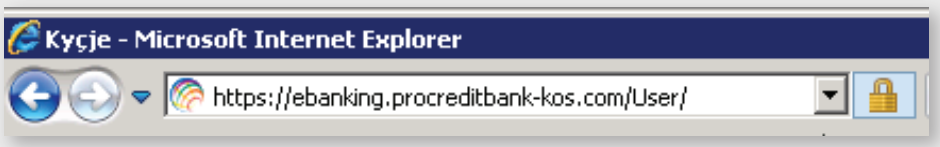
Za više informacija uvek možete posetiti specijalizovane veb lokacije kao što su:
http://www.banksafeonline.org.uk/faq.html

Dodatne zaštitne mere

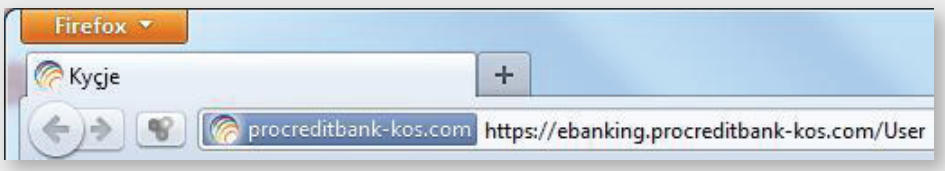
- Uvek zapamtite svoju lozinku i druge bezbednosne informacije, a zatim uništite obaveštenje koje sadrži te podatke što je pre moguće.
- Nikada nemojte zapisivati ili snimati lozinku ili druge bezbednosne informacije, osim ako nisu dobro prikrivene.
- Uvek se pridržavajte uslova i odredbi svoje banke.
- Uvek preduzimajte razumne korake kako biste svoju lozinku i druge bezbednosne informacije držali u tajnosti u svakom trenutku - nikada ih nemojte otkrivati porodici ili prijateljima.
- Nemojte koristiti istu lozinku koju koristite za mrežno bankarstvo na bilo kojim nebankarskim sajtovima.
- Ako promenite lozinku, izaberite onu koju nije lako pogoditi.
- Nikada nikome ne dajte podatke o svom nalogu ili bezbednosne podatke. Ako zovete banku, budite svesni koje informacije će od vas tražiti: obično nećete tražiti potpunu lozinku.
- Uvek koristite sigurnu uslugu e-bankarstva ProCredit Bank. Uvek idite direktno na veb lokaciju upisivanjem [https://ebanking.procreditbank-kos.com]. Uverite se da se u donjem desnom uglu prozora pregledača nalazi zaključani katanac ili neprekinuti ključ pre nego što pristupite veb lokaciji banke.
- Početak internet adrese banke će se promeniti sa 'http' u 'https' kada se uspostavi sigurna veza.
- Proverite da li je simbol sigurne veze vidljiv.
- Sigurnosni sertifikat veb stranice ProCredit Bank možete proveriti klikom na bravu koja se pojavljuje u vašem pregledaču.

Internet Explorer 9

Internet Explorer 8



Firefox 4



ProCredit Bank

e-Banking

- Svaki izuzetak od uobičajene rutine u vezi sa vašim Internet bankarstvom treba tretirati kao sumnjiv. Ako imate bilo kakvih nedoumica, kontaktirajte ProCredit Bank tako što ćete posetiti najbližu poslovnicu, kontaktirati savetnika za klijente ili nazvati našu liniju za pomoć: [+383-38 / 555-555 ili +383-49 / 555- 555]
- Nikada ne ostavljajte računar bez nadzora kada ste prijavljeni na Internet bankarstvo.
- Uverite se da ste se pravilno odjavili kada završite bankarstvo na mreži.

Više informacija o bezbednosti na mreži

Šta je phishing?

Phishing je naziv za praksu slanja e-pošte nasumično, navodno, od prave kompanije koja posluje na Internetu, u pokušaju da prevari klijente te kompanije da otkriju informacije na lažnoj veb stranici kojom upravljaju prevaranti. Ove e -poruke obično tvrde da je potrebno „ažurirati“ ili „verifikovati“ podatke o korisničkom nalogu i pozivaju ljude da kliknu na vezu u e -poruci koja ih vodi do lažne veb stranice. Sve informacije koje su unete na lažnu veb lokaciju će kriminalci prisvojiti u svoje lažne svrhe.

Kako mogu da izbegnem da postanem žrtva “phishing”?
Ključna stvar je ostati sumnjičav prema svim neželjenim ili neočekivanim e -porukama koje primite, čak i ako izgleda da potiču iz pouzdanog izvora. E-poruke se šalju potpuno nasumično u nadi da će doći do žive adrese e-pošte klijenta sa računom u banci na koju se cilja.

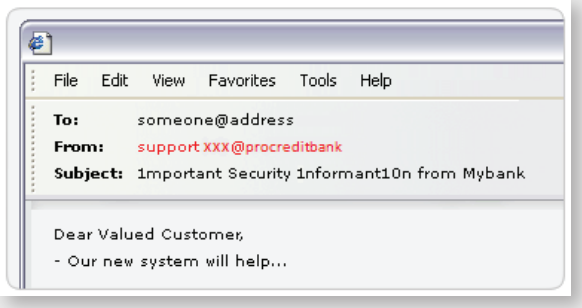
Iako vas ProCredit Bank može kontaktirati putem e -pošte, ProCredit banka vas nikada neće kontaktirati putem e -pošte da vas zamoli da unesete lozinku ili bilo koje druge osetljive podatke klikom na vezu i posetom veb stranici. Zaustavite se i razmislite kako vaša banka normalno komunicira s vama i nikada ne otkrivajte svoju potpunu lozinku ili bilo koje lične podatke.

ProCredit Bank

e-Banking

Kako uočiti phishing e -poštu

1 – Od koga je e-pošta?



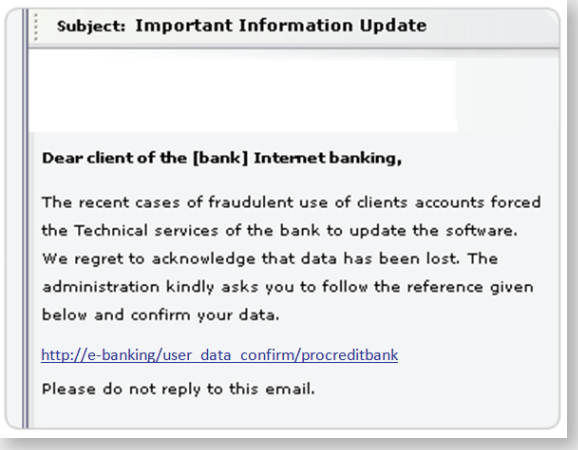
Imejlovi za krađu identiteta mogu izgledati kao da dolaze sa prave adrese e-pošte ProCredit Bank. Nažalost, zbog postavljanja internetske e-pošte, phisheri su relativno jednostavni da stvore lažni unos u polju "Od:".

Adresa e -pošte koja se pojavljuje u polju „Od:“ e-pošte NIJE garancija da je došla od osobe ili organizacije navedene u e-adresi. Ova e-pošta nije poslata korišćenjem sopstvenih sistema banke.

2 – Za koga je e-pošta?
E -poruke se nasumično šalju na masovne liste e-pošte i prevaranti gotovo sigurno neće znati vaše pravo ime ili zaista bilo šta drugo o vama, i obraćaće vam se u nejasnim terminima poput „Dragi cenjeni klijente".

3 – Pažljivije pogledajte e -poruku – da li izgleda „lažno“ "?

Prva stvar koju treba zapamtiti je da vam banke nikada neće pisati i tražiti vašu lozinku ili bilo koje druge osetljive podatke putem e-pošte. Poruka će takođe verovatno sadržavati čudne "reč1" ili vEliKa sLova u polju “Predmet:" (ovo je pokušaj zaobilaženja softvera za filtriranje neželjene pošte), kao i gramatičke i pravopisne greške.



Nikada se nemojte prijavljivati na svoj bankovni račun na mreži klikom na vezu u e-poruci. Uvek otvorite veb pregledač i sami unesite adresu veb stranice Internet bankarstva ProCredit Bank.

Ako imate bilo kakvih nedoumica u vezi sa valjanošću e-pošte koja bi trebalo da stigne od ProCredit banke, molimo vas da o tome odmah obavestite ProCredit banku tako što ćete posetiti najbližu poslovnicu, kontaktirati svog savetnika za klijente ili nazvati sledeći broj [+383-38 / 555-555 ili +383-49 / 555-555]. Sumnjivu e-poruku možete proslediti i na sledeću adresu e-pošte [abuse@procreditbank-kos.com].

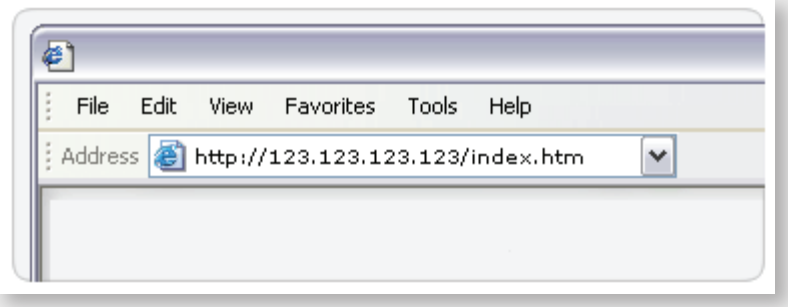
4 - Kuda vodi taj hiperlink?
Nažalost, previše je lako prikriti pravo odredište veze, tako da se prikazana veza i sve što se prikaže na statusnoj traci vašeg programa za e-poštu može lako falsifikovati.

ProCredit Bank

e-Banking

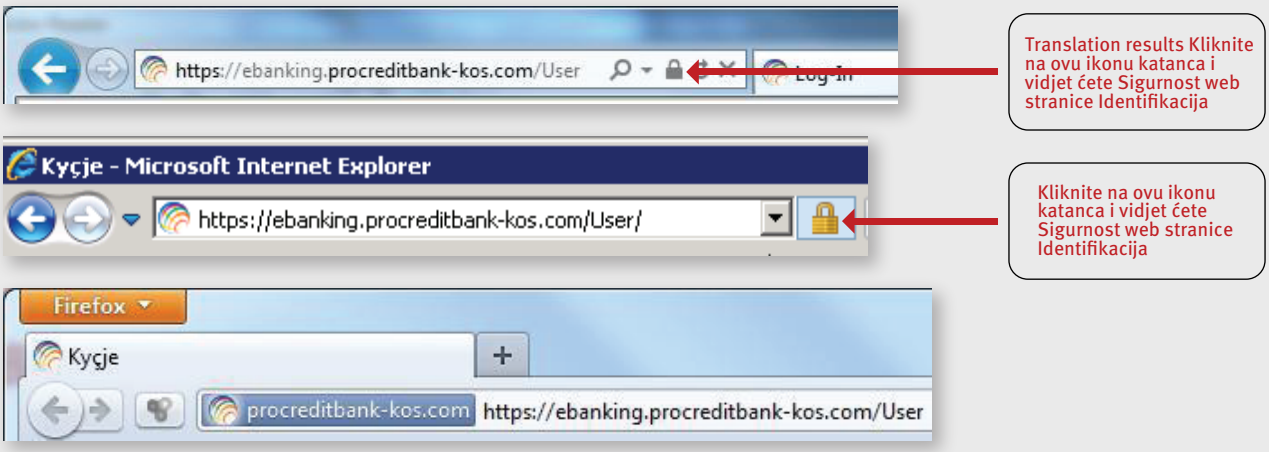
Kako uočiti phishing veb lokaciju

Koja je adresa veb lokacije?



Ako posetite veb lokaciju nakon što kliknete na vezu u e-poruci, postoji mnogo načina da prikrijete pravu lokaciju lažne veb lokacije u traci za adresu. Adresa veb lokacije može početi sa imenom domena originalne veb lokacije, ali to nije garancija da vodi do prave lokacije. Ostali trikovi uključuju korišćenje numeričkih adresa, registraciju slične adrese (kao što je npr www.mybank- verify.com), ili čak umetanje lažne trake za adresu u prozor pregledača. Mnoge veze sa ovih stranica možda zaista idu na originalnu veb lokaciju, ali nemojte se zavaravati.

Možete potvrditi da ste na zaštićenoj službenoj veb lokaciji ProCredit Banke upoređivanjem simbola sigurne veze



Sigurnosni sertifikat veb stranice ProCredit Bank možete proveriti klikom na bravu koja se pojavljuje u vašem pregledaču.

Čuvajte se lažnih iskačućih prozora

Umesto prikazivanja potpuno lažne veb lokacije, prevaranti mogu učitati originalnu veb lokaciju u glavni prozor pregledača, a zatim postaviti veći deo lažnog iskačućeg prozora. Ako se to bude prikazalo na ovaj način, vi ćete moći sa vidite adresnu traku stvarne veb lokacije u pozadini, iako će sve informacije koje unesete u iskačući prozor biti prikupljene od strane prevaranata za njihovu upotrebu.

ProCredit Bank

e-Banking

Da biste pristupili svom bankovnom računu na mreži, sami unesite adresu u novi prozor. Adresa vašeg pravog veb sajta za onlajn bankarstvo počinje sa „https“ i uključivaće mali katanac na dnu prozora pregledača.

Prijavljivanje sumnjivih imejlova
Ako primite sumnjivu poruku e-pošte, odmah obavestite ProCredit Bank tako što ćete posetiti najbližu poslovnicu, kontaktirati svog savetnika za klijente ili nazvati sledeći broj [+383-38 / 555-555 ili +383-49 / 555-555]. Vi takođe možete da prosledite e-poruku i na sledeću adresu e -pošte [abuse@procreditbank-kos.com].

Upamtite:

- Banke vam nikada neće poslati e -poruku sa zahtevom da "potvrdite" ili "ažurirate" lozinku ili bilo koje lične podatke klikom na vezu i posetom veb lokaciji
- Oprezno postupajte sa svim neželjenim e-porukama i nikada nemojte kliknuti na veze u takvim e-porukama niti unositi bilo kakve lične podatke
- Da biste se prijavili na Internet bankarstvo, otvorite veb pregledač i sami unesite adresu
- Ako sumnjate u valjanost e-pošte ili mislite da ste možda otkrili poverljive informacije, molimo vas da o tome odmah obavestite ProCredit banku tako što ćete posetiti najbližu poslovnicu, kontaktirati svog savetnika za klijente ili nazvati sledeći broj [+383-38 / 555-555 ili +383 - 49 / 555-555]. Vi takođe možete da prosledite e-poruku i na sledeću adresu e -pošte [abuse@procreditbank-kos.com].

Podsetnik:

- Oprezno postupajte sa svim neželjenim e -porukama (posebno onima od nepoznatih pošiljalaca) i nemojte nikada da kliknite na veze u takvim e -porukama da biste posetili nepoznate veb lokacije
- Instalirajte antivirusni softver, ažurirajte ga i redovno izvršavajte bezbednosna skeniranja
- Instalirajte i naučite kako da koristite lični zaštitni zid
- Instalirajte najnovija bezbednosna ažuriranja, poznata i kao patches