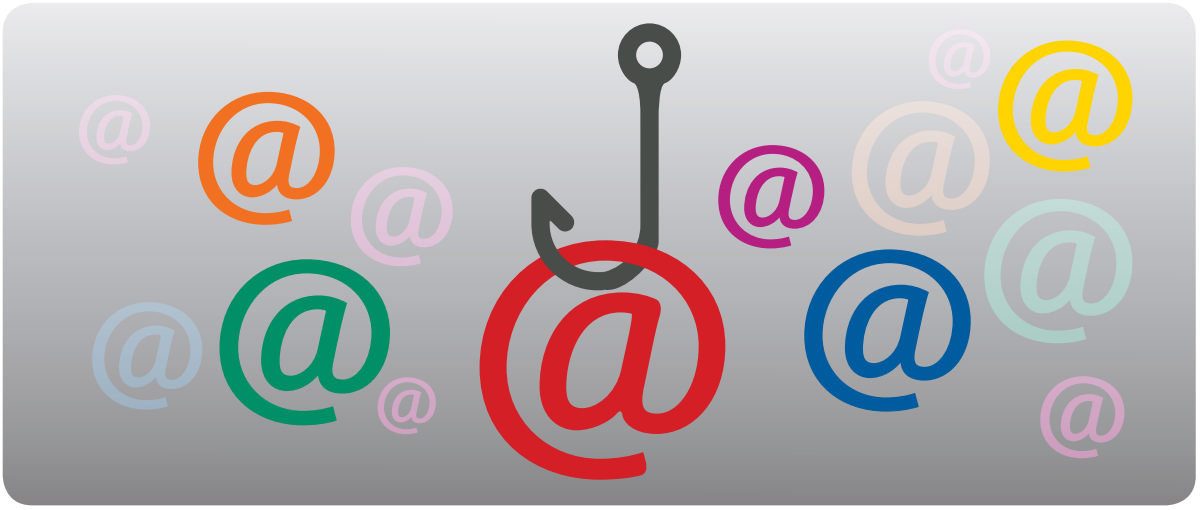
Part of the ProCredit Group

ProCredit Bank

Kako se mogu zaštititi od „phishinga“?

ProCredit Bank se obavezala da Vaše online transakcije učini sigurnim i da zaštiti integritet podataka Vašeg bankovnog računa. Da bi to postigli, koristimo najmoderniji sigurnosni software i provodimo različite sigurnosne procedure. Međutim, uvijek trebate biti svjesni da se internet i e-mail mogu koristiti kao sredstva za nezakonitu aktivnost. Zbog toga vam preporučujemo da poduzmete određene jednostavne mjere predostrožnosti da se osigurate prilikom obavljanja vaših bankarskh poslova online.



Savjeti kako izbjeći „phishing“

- **Šta je „phishing“ (mrežna krađa identiteta)?**

  „Phishing“ predstavlja pokušaj da se pristupi osjetljivim ličnim podacima slanjem e-mailova koji navodno dolaze od stvarne kompanije koja djeluje na internetu, ali se zapravo radi o lažnoj web stranici koju održavaju prevaranti.

- **Koje će se informacije od mene tražiti?**

  U „phishing“ e-mail-ovima se obično tvrdi da je neophodno „ažurirati“ ili „potvrditi“ informacije o vašem računu, te se klijenti nagovaraju da kliknu na dati link u e-mail-u koji ih vodi do lažne web stranice. Sve informacije koje upišete u lažnu web stranicu dospijevaju u ruke kriminalaca koje oni zatim koriste u svoje nezakonite svrhe.

- **Kako mogu izbjeći da postanem žrtva “phishing-a”?**

  Ključna stvar vaše zaštite je da imate određenu dozu sumnje prema svim neželjenim ili neočekivanim e-mail-ovima koje primite, čak i kada se čini da potiču iz povjerljivog izvora. Ti e-mail-ovi se šalju u nadi da će stići na aktivnu elektronsku adresu klijenta sa računom u ciljanoj instituciji.

- **Šta trebam uraditi ako primim phishing e-mail?**

  Ako primite sumnjiv e-mail, molimo Vas da odmah obavijestite ProCredit Bank posjetom najbližoj poslovnici, kontaktiranjem Vašeg službenika za bankarske usluge ili pozivom na slijedeći brojeve: **+387 33 253 993** ili **+387 61 228 527**.
  Pored toga možete proslijediti e-mail na slijedeću adresu: **probanking@procreditbank.ba.**

Za više informacija pogledajte sadržaj na stručnim web stranicama poput
http://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing

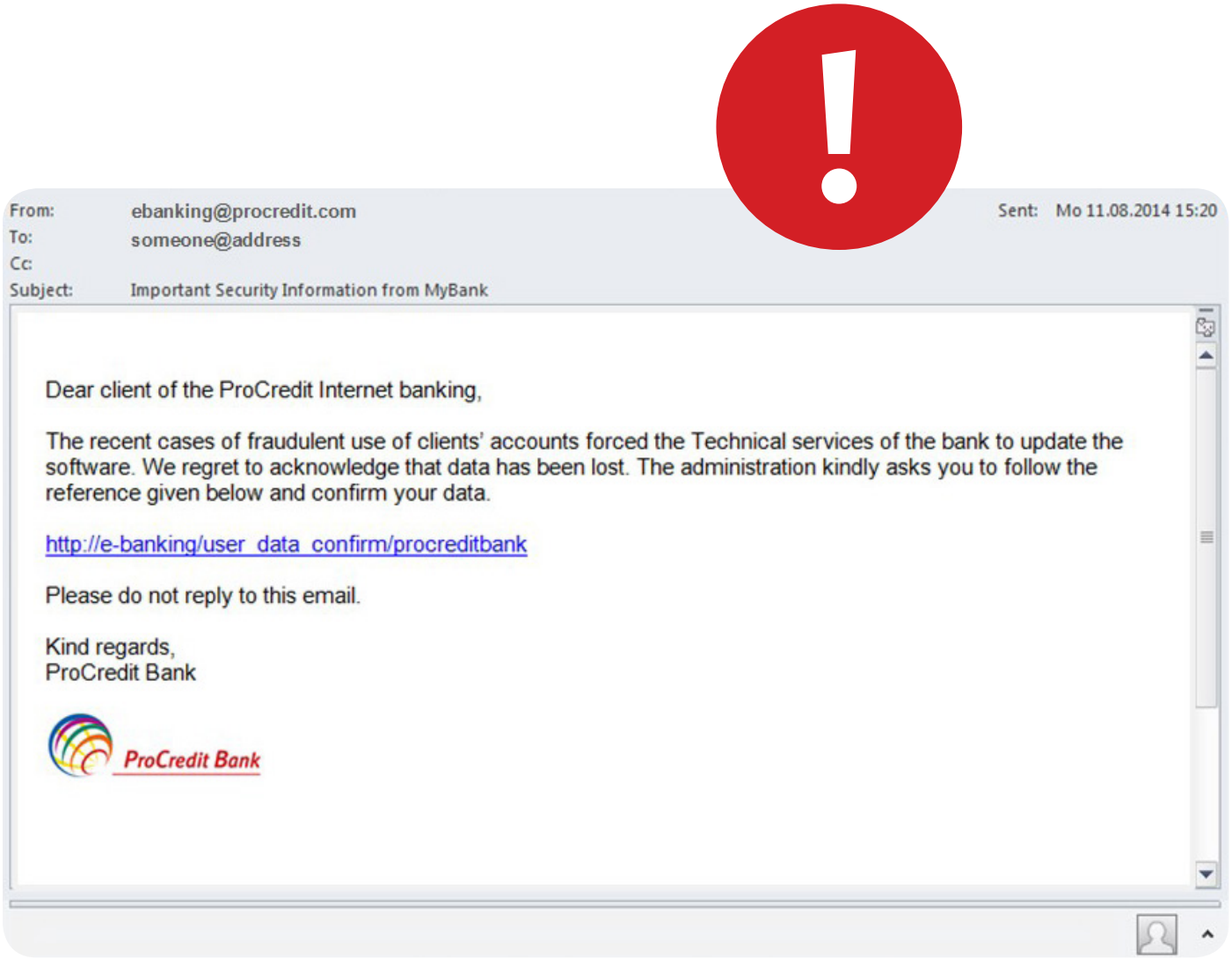
Part of the ProCredit Group

ProCredit Bank

Dodatni savjeti o online sigurnosti

Kako ću primjetiti „phishing“ e-mail?

„Phishing“ e-mailovi mogu izgledati kao da dolaze sa službene ProCredit Bank e-mail adrese. Nažalost, „fišeri“ mogu relativno lako kreirati lažne podatke u polje “Od” i sakriti stvarnu destinaciju linka.



From: ebanking@procredit.com
Sent: Mo 11.08.2014 15:20
To: someone@address
Cc:
Subject: Important Security Information from MyBank

Dear client of the ProCredit Internet banking,

The recent cases of fraudulent use of clients' accounts forced the Technical services of the bank to update the software. We regret to acknowledge that data has been lost. The administration kindly asks you to follow the reference given below and confirm your data.

http://e-banking/user_data_confirm/procreditbank

Please do not reply to this email.

Kind regards,
ProCredit Bank

ProCredit Bank

Premda vas ProCredit Bank može kontaktirati e-mail-om, taj e-mail nikad neće sadržavati link koji vas upućuje na web stranicu koja od vas traži vaše lične podatke (password, šifru tokena, itd.).

Posumnjajte u svaku promjenu Vaše redovne rutine u internet bankarstvu. Ako imate bilo kakve nedoumice, molimo Vas da kontaktirate ProCredit Bank posjetom Vašoj najbližoj poslovnici, kontaktiranjem Vašeg službenika za bankarske usluge ili pozivom na:

+387 33 253 993 ili +387 61 228 527.