## Informata për Sigurinë Online

**ProCredit Bank është e zotuar për mbrojtjen e integritetit të transaksioneve dhe detajeve të llogarisë suaj. Për këtë arsye, ProCredit Bank përdor softuerët dhe procedurat më të reja të sigurisë për të mbrojtur transaksionet tuaja online. Megjithatë, ju gjithnjë duhet të jeni të vetëdijshëm se Interneti dhe posta elektronike (e-maili) mund të përdoren si mjete për aktivitete ilegale, prandaj ne ju rekomandojmë që të ndërmerrni disa masa të thjeshta për të forcuar sigurinë e përdorimit të tyre.**

## Udhëzime për të ruajtur sigurinë online

**Informohuni se me kë keni të bëni**

Gjithmonë qasjuni Internetit duke shkruar adresën e bankës në shfletuesin tuaj të internetit [**https://ebanking.procreditbank-kos.com**]. Asnjëherë mos u drejtoni në ueb faqe nga ndonjë vegëz në një postë elektronike (e-mail) si dhe mos i futni të dhënat tuaja personale. Nëse keni dyshime kontaktoni ProCredit Bank-ën në: [**+381-38 / 555-555 apo +386 - 49 / 555-555**].

**Mbajini me kujdes fjalëkalimet dhe NPI-të (PIN)**

Gjithmonë keni kujdes nga posta elektronike (e-maili) e padëshiruar ose thirrjet e dyshimta të cilat kërkojnë nga ju që të shpalosni çfarëdo detaje personale apo numra të kartelës. Mbani këto informata të fshehta. Jini të kujdesshëm për dhënien e informatave personale dikujt që nuk e njihni. Banka juaj dhe policia asnjëherë nuk do t'ju kontaktonin për t'ju kërkuar shpalosjen e informatave të NPI-së (Numri Personal Identifikues) ose fjalëkalimit.

**Ruajini paratë tuaja!**

Mos u mashtroni nga posta elektronike (e-maili) e cila tingëllon e sinqertë dhe e cila ju ofron mundësi që lehtë të bëni para. Nëse duket ofertë shumë e mirë për të qenë e vërtetë, me siguri se nuk është e tillë ! Posaçërisht keni kujdes nga posta elektronike që mund të vije nga jashtë vendit – do të jetë shumë më vështirë të kontrollohet nëse dërguesit janë ata të cilët pretendojnë se janë.

**Mbrojeni kompjuterin tuaj personal - KP (PC)**

Përdorni softuer anti-virus të azhurnuar dhe një mur mbrojtës (firewall) personal, nëse kompjuteri juaj përdor sistemin operativ Microsoft Windows, azhurnojeni

nëpërmjet ueb faqes së Microsoft. Gjithmonë përdorni versionin më të ri të shfletuesit të Internetit i cili përmban të gjitha azhurnimet e sigurisë. Jini shumë të kujdesshëm nëse përdorni Internet kafetë, bibliotekat ose ndonjë KP i cili nuk është i juaji dhe mbi të cilin nuk keni kontroll.

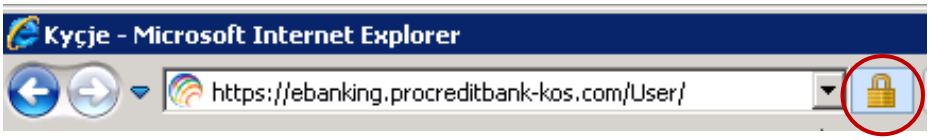
**Për më shumë informata ju gjithmonë mund të vizitoni ueb faqet e specializuara si p.sh.:http://www.banksafeonline.org.uk/faq.html**

## Masat mbrojtëse shtesë

- Gjithmonë mbani në mend fjalëkalimin dhe informatat tjera të sigurisë dhe pastaj, nëse këto informata i keni të shkruara diku, sa më parë që është e mundur shkatërroni njoftimin i cili përmban këto informata.
- Asnjëherë mos shkruani ose regjistroni diku fjalëkalimin tuaj ose informatat tjera të sigurisë, përveç nëse janë maskuar mirë.
- Sigurohuni që gjithmonë të zbatoni udhëzimet dhe kushtet e përdorimit të rekomanduara nga banka .
- Gjithnjë merrni hapa të arsyeshëm të mbani fshehtë fjalëkalimin tuaj dhe informatat tjera të sigurisë gjatë tërë kohës – asnjëherë mos i tregoni ato familjes ose shokëve.
- Mos përdorni fjalëkalimin e njëjtë për shërbimet bankare online në ndonjë faqe tjetër jo bankare.
- Nëse e ndërroni fjalëkalimin, zgjedhni një i cili nuk mund të qëllohet lehtë.
- Asnjëherë mos jepni detajet e llogarisë suaj ose informatat e sigurisë ndokujt. Nëse i telefononi bankës, keni kujdes se çfarë informata ju kërkojnë ata: zakonisht nuk ju kërkohet fjalëkalimi i plotë.
- Sigurohuni që gjithnjë të përdorni shërbimin e **sigurt e-banking të ProCredit Bank-ës.** Gjithmonë shkoni drejtpërdrejtë në ueb faqe duke shkruar [**https://ebanking.procreditbank-kos.com**]. Sigurohuni që të jetë i paraqitur dryni i mbyllur ose çelësi i pathyer në pjesën e poshtme të djathtë të dritares së shfletuesit tuaj para se t'i qaseni ueb faqes së bankës. Fillimi i ueb adresës së bankës do të ndryshoj nga 'http' to 'https' kur bëhet lidhja e sigurt.
- Kontrolloni nëse simboli i lidhjes së sigurt është i dukshëm.
- Ju mund të kontrolloni **Certifikatën e Sigurisë (Security Certificate)** të ueb faqes së ProCredit Bank-ës duke klikuar në drynin i cili paraqitet në shfletuesin tuaj .

**Shfletuesi i Internetit 9**


**Shfletuesi i Internetit 8**




**Firefox 4**


- **Çfarëdo** ndryshimi që vërehet në pamjen e zakonshme të faqes së shërbimeve bankare përmes internetit duhet të trajtohet si i dyshimtë. Nëse keni ndonjë dyshim, ju lutemi kontaktoni ProCredit Bank-ën duke vizituar degën më të afërt, duke kontaktuar këshilltarin për klient ose duke telefonuar në linjën e ndihmës: [**+381-38 / 555-555 apo +386 - 49 / 555-555**]

- Asnjëherë mos e lini kompjuterin tuaj pa mbikëqyrje kur jeni të kyçur në shërbimin bankar përmes Internetit.
- Sigurohuni që të shkyçeni si duhet kur të përfundoni përdorimin e shërbimeve bankare online.

# Më shumë informata për sigurinë online

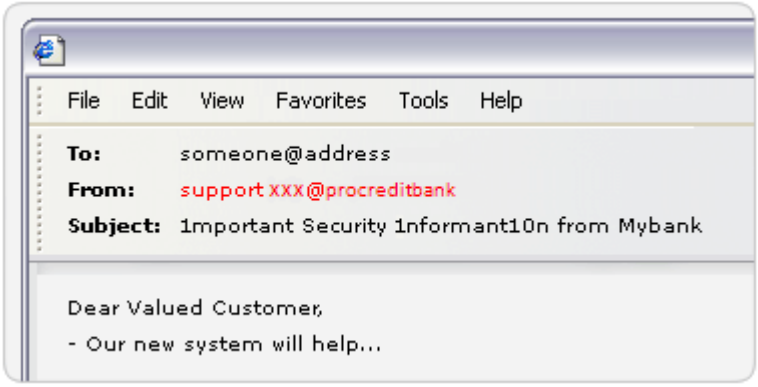
**Çka është phishing?**
Phishing është emri i cili i është dhënë praktikës së të dërguarit të postave elektronike (e-mailëve) të rastësishme me pretendim se ato vijnë nga një kompani e vërtetë e cila operon në Internet, në përpjekje për të mashtruar konsumatorët e asaj kompanie duke shpalosur kështu informatat në ueb faqe false të operuar nga mashtruesit. Këto posta elektronike zakonisht pretendojnë se është e nevojshme të "azhurnohen" ose "verifikohen" informatat e llogarisë së konsumatorit dhe ato nxisin njerëzit që të klikojnë në një vegëz në postën elektronike e cila i dërgon ata në ueb faqen false. Çfarëdo informate e cila futet në ueb faqen false do të merret nga kriminelët për qëllimet e tyre mashtruese.

**Si mund ta parandalojë që të mos bëhem viktimë e phishing?**
Gjëja kryesore është të keni kujdes për të gjitha postat elektronike (e-mailët) të dyshimta dhe të papritura të cilat pranoni, edhe nëse ato duken në shikim të parë se vijnë nga një burim i besueshëm. Këto posta elektronike dërgohen tërësisht në baza të rastësishme duke shpresuar që të arrijë një adresë të postës elektronike aktive të një konsumatori me një llogari në bankën e synuar për sulm.

Edhe pse ProCredit Bank mund t'ju kontaktojë përmes postës elektronike (e-mailit), ProCredit Bank asnjëherë nuk do t'ju kërkojë përmes postës elektronike të futni fjalëkalimin tuaj ose informatat tjera të ndjeshme duke klikuar në një vegëz si dhe duke vizituar një ueb faqe. Rikujtohuni se si banka juaj zakonisht komunikon me ju dhe asnjëherë mos shpalosni fjalëkalimin tuaj të plotë ose ndonjë informatë personale.

**Si të dallohet një postë elektronike phishing**

**1 – Prej kujt është kjo postë elektronike?**

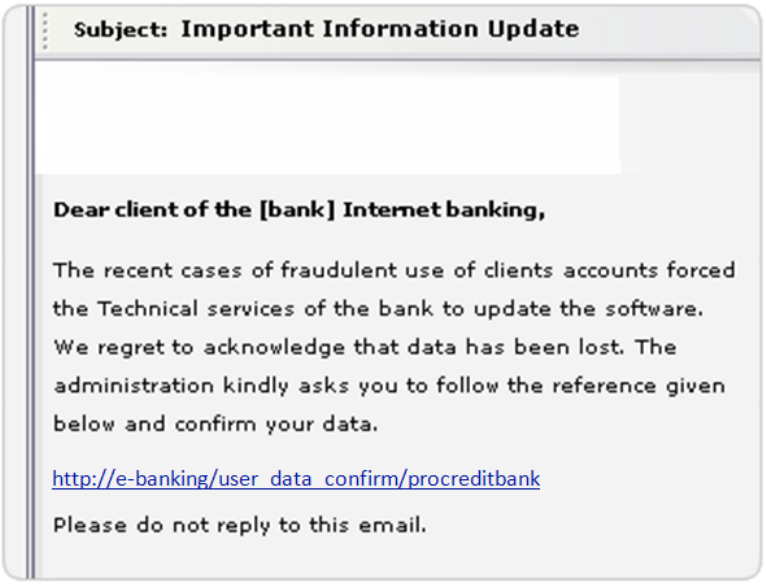



Postat elektronike phishing mund të duken sikurse vijnë nga një postë elektronike (e-mail) reale e ProCredit Bank-ës. Fatkeqësisht për shkak të përcaktimit të postës elektronike në Internet, është relativisht e thjeshtë për "phisheret" të krijojnë një hyrje false në fushën "Nga:" ("From:").

Adresa e postës elektronike e cilat duket në fushën “Nga:” (“From:”) të një poste elektronike NUK është vërtetim se ajo vjen nga personi ose organizata e deklaruar në adresën e postës elektronike. Këto posta elektronike nuk janë dërguar duke përdorur sistemet e vetë bankës.

**2 – Për kë është kjo postë elektronike?**
Postat elektronike (e-mailët) dërgohen rastësisht në një listë të madhe të adresave dhe mashtruesit me siguri se nuk do të dinë emrin tuaj real dhe ndonjë gjë tjetër për ju, dhe do t'ju drejtohen në mënyrë të përgjithshme si "I Nderuari Konsumator i Çmuar", dhe jo duke ju drejtuar me emërin tuaj personal.

**3 – Vëreni me kujdes postën elektronike – a duket si "phishing"?**
Gjëja e parë për tu mbajtur ndër mend është se banka jonë asnjëherë nuk do t'ju shkruajë për t'ju kërkuar fjalëkalimin ose informatat tjera të ndjeshme përmes postës elektronike (e-mailit). Porosia është e mundur të përmbajë tekste të "paz11konshme" ose "shkroNJa të MëDHa" në fushën e "Titullit:" ("Subject:") (kjo është përpjekje për të anashkaluar softuerin për filtrimin e spamit), si dhe gabime gramatikore dhe të drejtshkrimit.


Subject: Important Information Update

Dear client of the [bank] 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.

Shembull i postës elektronike mashtruese

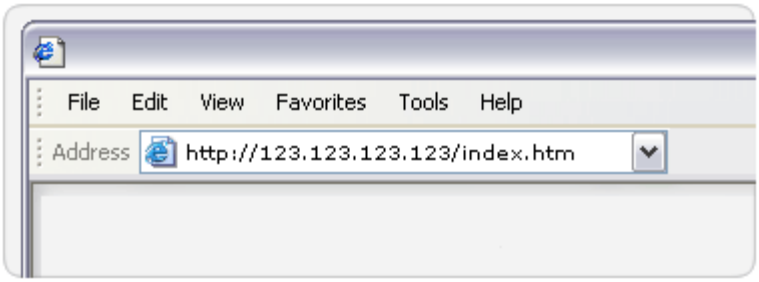
**Asnjëherë** mos u kyçni në llogarinë e shërbimit bankar online duke klikuar në një vegëz në një poste elektronike. **Gjithnjë** hapeni shfletuesin tuaj të internetit dhe shkruani adresën e ProCredit Bank-ës për shërbime bankare.

Nëse keni dyshime për vlefshmërinë e një poste elektronike (e-maili) e cila pretendon se vjen nga ProCredit Bank, ju lutemi menjëherë njoftoni ProCredit Bank-ën duke vizituar degën më të afërt, duke kontaktuar këshilltarin tuaj për klient ose duke telefonuar në numrin vijues [**+381-38 / 555-555 apo +386 - 49 / 555-555**]. Ju gjithashtu mund të përcillni postën elektronike të dyshimtë në adresën vijuese të postës elektronike [**abuse@procreditbank-kos.com**].

**4 – Ku shkon ajo vegëz?**
Fatkeqësisht, është shumë e lehtë të maskohet destinomi real i një vegëze, ashtu që vegëza e paraqitur dhe gjithçka që paraqitet në rreshtin e statusit të programit tuaj për postë elektronike mund të falsifikohet lehtësisht.

**Si të dallohet një ueb faqe Phishing**

Çka është adresa e faqes?



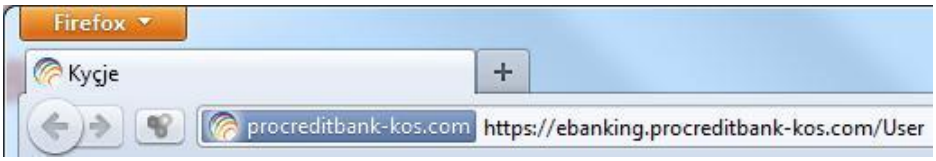

Nëse vizitoni një ueb faqe pas klikimit në një vegëz në një postë elektronike (e-mail), ka shumë mënyra për të fshehur lokacionin e vërtetë të asaj ueb faqeje në rreshtin e adresës. Adresa e faqes mund të fillojë me emrin e vërtetë të domenit të faqes, por nuk ka garancion se ajo të dërgon te faqja e vërtetë. Dredhitë tjera përfshijnë përdorimin e adresave numerike, regjistrimin e adresave të ngjashme (si **www.mybank-verify.com**), madje edhe futjen e rreshtit të adresave të falsifikuar në dritaren e shfletuesit. Shumë nga vegëzat nga këto faqe realisht mund të shkojnë në ueb faqe të vërteta, megjithatë, mos u mashtroni.

Ju mund të konfirmoni se jeni në ueb faqen zyrtare të sigurt të ProCredit Bank-ës duke krahasuar simbolin e lidhjes së sigurt.

**Shfletuesi i Internetit 9**


**Shfletuesi i Internetit 8**


**Firefox 4**




Ju mund të kontrolloni **Certifikatën e Sigurisë (Security Certificate)** duke klikuar në drynin i cili paraqitet në shfletuesin tuaj.

**Keni kujdes nga dritaret dalëse mashtruese**

Në vend të paraqitjes së një faqe tërësisht false, mashtruesit mund të paraqesin ueb faqen e vërtetë në dritaren kryesore të shfletuesit dhe pastaj të vendosin një faqe tjetër dalëse që mbulon shumicën e faqes tjetër. Nëse paraqitet në këtë mënyrë, ju do të jeni në gjendje të shihni rreshtin e adresës së ueb faqes reale në prapavijë, edhe pse informatat të cilat ju shkruani në dritaren dalëse do të mblidhen nga mashtruesit për përdorim nga ta.

Për tu kyçur në llogarinë tuaj për shërbime bankare online, shkruari vetë adresën në një dritare të re. Adresa reale e ueb faqes së shërbimit bankar online do të fillojë me “https” dhe të përfshijë një dry të vogël në fund të dritares së shfletuesit.

**Raportimi i postës elektronike të dyshimtë**

Nëse pranoni një postë elektronike (e-mail) të dyshimtë, ju lutemi menjëherë njoftoni ProCredit Bank-ën duke vizituar degën tuaj më të afërt, duke kontaktuar këshilltarin tuaj për klient ose duke telefonuar në numrin vijues [**+381-38 / 555-555 apo +386 - 49 / 555-555**]. Ju gjithashtu mund të përcillni postën elektronike të dyshimtë në adresën vijuese të postës elektronike [**abuse@procreditbank-kos.com**].

**Mbani në mend:**

- Bankat asnjëherë nuk do t'ju ju shkruajnë postë elektronike (e-mail) për të kërkuar nga ju të "konfirmoni" ose "azhurnoni" fjalëkalimin tuaj ose ndonjë informatë personale duke klikuar në një vegëz dhe duke vizituar një ueb faqe.
- Trajtoni të gjithë postën elektronike të padëshiruar me kujdes dhe asnjëherë mos klikoni në vegëza në postat tilla elektronike ose vendosni ndonjë informatë personale.
- Për tu kyçur në shërbimin bankar përmes Internetit, hapeni shfletuesin tuaj të internetit dhe shkruajeni vetë adresën.
- Nëse keni dyshime për vlefshmërinë e një poste elektronike, ose nëse mendoni se keni shpalosur informata konfidenciale, ju lutemi menjëherë njoftoni ProCredit Bank-ën duke vizituar degën më të afërt, duke kontaktuar këshilltarin tuaj për klient ose duke telefonuar në numrin vijues [**+381-38 / 555-555 apo +386 - 49 / 555-555**]. Ju gjithashtu mund të përcillni postën elektronike të dyshimtë në adresën vijuese të postës elektronike [**abuse@procreditbank-kos.com**].

**Përkujtim:**

- **Trajtoni me kujdes të gjitha postat elektronike (e-mailët) të padëshiruara (posaçërisht ato nga dërguesit e panjohur) dhe asnjëherë mos klikoni në vegëza në postat elektronike të tilla për të vizituar ueb faqet e panjohura**
- **Instaloni softuer anti-virus, mbani atë të azhurnuar dhe rregullisht bëni skenime të sigurisë**
- **Instaloni dhe mësoni se si të përdorni murin mbrojtës (firewall) personal**
- **Instaloni azhurnimet më të reja të sigurisë në sistemin operativ, gjithashtu të njohura si arnime (patches)**