Këshilla mbi masat e sigurisë në përdorimin e shërbimit NLB Klik " E-BANKING"

Për të hyrë në shërbimet bankare, në internet klientët duhet të hapin "UEBFAQEN" e sigurt dhe të certifikuar të NLB Prishtina e cila është: www.banka-ks.com/nlb

Në mënyrë që përdorimi i internetit të jetë i sigurt, është e rëndësishme të ndërmerren këto masa:

1. Mbrojtja e të dhënave personale si (Shfrytëzuesi , Parulladhe Kodi në pajisjenTOKEN)

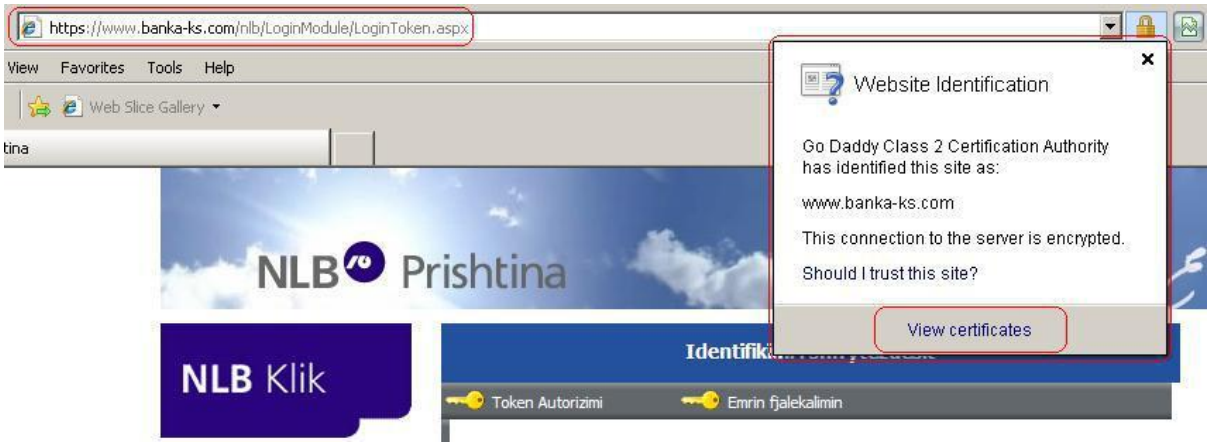
- Mbani mend **Shfrytëzuesin** dhe **Parullën**, ndërroni shpesh këto të fundit, dhe sigurohuni që të mos jenë lehtë të qëllueshme, p.sh. mos përdorni fjalë që gjenden në fjalorë, emra të qyteteve, emra të anëtarëve të familjes, ose datëlindjet.
- Mbani mend **Parullën**tuaj, në vend se ta shkruani atë dhe ta ruani në një copë letër.
- Nëse **Parullën**të shkruar vendosni ta ruani, atëherë ky informacion i ndjeshëm duhet të ruhet në një vend të sigurt.
- Si informacione të ndjeshme që janë: **Shfrytëzuesin** dhe **Parullën**mos e ndani me askënd.

2. Mbrojtja nga mashtrimi i mundshëm

- Bankat dhe institucionet financiare nganjëherë janë pre e të ashtuquajturës mashtrimi "PHISHING" e që donë të thotë përpjekje për mashtrim. Kjo është një formë e mashtrimit në internet ku klientët mashtrohen duke i zbuluar informacione KONFIDENCIALE një UEBFAQEJE mashtruese pra përdoruesve mashtrues. **Një shembull: kur dikush paraqitet si përfaqësues i bankës, i cili dërgon porosi elektronike apo thërret klientët duke kërkuar informacione si: Shfrytëzuesin, Parullën apo Kodin e paraqitur në Pajisjen TOKEN. Ne ju sigurojmë se përfaqësuesit NLB Prishtina, kurrë nuk do të kërkojnë informacione të tilla përmes postës elektronike apo telefonit, andaj të jeni t**ë vëmendshëm.
- Një rast tjetër i PHISHING Mashtrimit është kur një përdorues mashtrues klonon një UEBFAQE që ngjan me UEBFAQEN e www.banka-ks.com/nlb. Për t'ju shmangur një rreziku të tillë ju duhet të kujdeseni që jeni duke përdorur UEBFAQEN e dhënë nga NLB Prishtina. Kur të hyni në faqen e **NLB Klik**, në sistemin bankar në internet, para se të shkruani të dhënat tuaja sigurohuni se po filloni sesion të sigurt (SSL i koduar) i cili fillon me **HTTPS://** si në **Fig. 1**. Pastaj ju duhet të hyni në faqen e sigurt dhe të verifikoni certifikatën e sigurisë. Për tu siguruar që jeni duke komunikuar me sistemin bankar të NLB Prishtina ju duhet të klikoni në drynin e paraqitur si në **Fig. 1**,informatat e paraqitura do të ju shërbejnë për të verifikuar certifikatën e sigurisë që ju është dhënë nga Kompania,në rastin tonë aktualisht është **(2048 bit - Secure Certification Authority)** dhe me kujdes të shikoni vlefshmërinë e certifikatës, si në **Fig. 2.**

Kontrollimi i URL Adresës e cila është: www.banka-ks.com/nlb

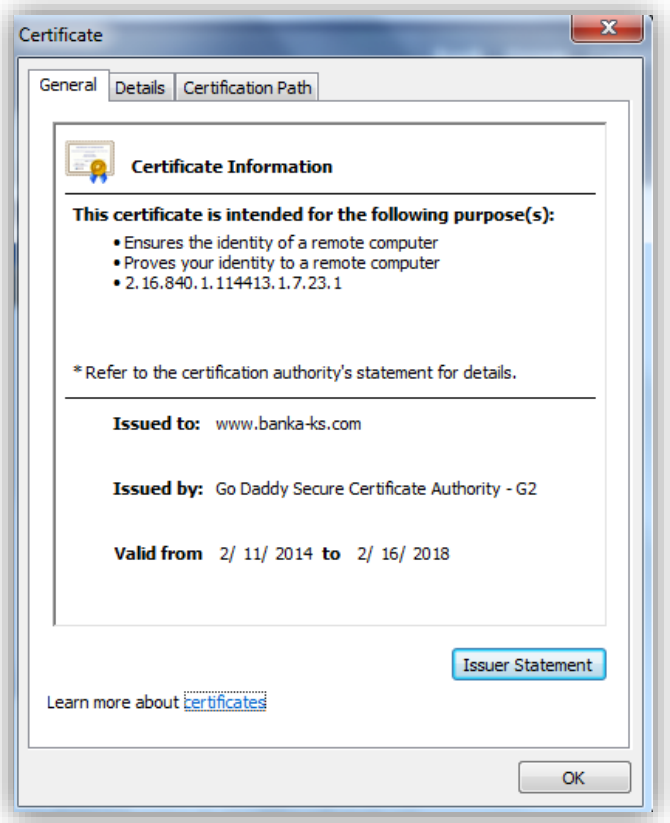
Fig. 1



Duke klikuar në **VIEW CERTIFICATES**, nga **Fig. 1**, do të hapet faqja si në **Fig. 2**, e cila ju mundëson kontrollimin e detajeve të certifikatës të cilat janë te renditura më poshtë:

1. **Lëshuar për** https://www.banka-ks.com
2. **Lëshuar nga**"GoDaddySecureCertificationAuthority"
3. **Vlefshmëria nga:**2/11/2014 **deri më** 2/16/2018

Fig



3. Mbrojtja e kompjuterit

- Pasi të keni qasje në lidhje të internetit, është e rëndësishme që kompjuterin tuaj ta mbroni nga qasja e personave te paautorizuar ose programet e rrezikshme

- (UEBFAQE të dyshimta, fotografi te dyshimta, viruse, e-mailë e të tjerë). Në kompjuterin tuaj është e rëndësishme të keni të instaluar programet ANTI-VIRUS, FIREWALL dhe ANTI-SPYWARE që mund të vijnë me kompjuterin tuaj apo janë dhënë nga ofruesi i shërbimit të Internetit. Programi FIREWALL mbron kompjuterin nga sulmet malicioze nga jashtë, dhe ka ngjashmëri me programin ANTI-VIRUS. SPYWARE është një program që është i instaluar në kompjuterin tuaj pa dijeninë tuaj dhe ai mban gjurmët e veprimeve tuaja (parullave, kodeve, etj.) gjatë përdorimit të kompjuterit dhe internetit. Prandaj është i nevojshëm një program ANTI -SPYWARE për të mbrojtur kompjuterin nga këto sulme. Sigurohuni që këto programe të azhurnohen rregullisht.

- Përdorimi i sistemit bankar në një kompjuter publik nuk këshillohet, pasi që është e vështirë të dihet se sa të siguruar janë këta kompjuterë.

- Mundësisht përdorni versionin më të ri të shfletuesit të internetit, i cili përfshin të gjitha informatat më të reja të sigurisë. Me furnizuesin tuaj të rrjetit kontrolloni rregullisht tek shfletuesit nëse është në dispozicion ndonjë informacion i ri i sigurisë.

- Me ofruesin tuaj të sistemit operativ,kontrolloni rregullisht nëse informacionet e sigurisë janë lëshuar në përdorim.

4. Informacione për tu konsideruar rreth TOKEN-it Fizik

- TOKEN-i është pajisje e sigurisë që përdoret për gjenerimin e kodeve për një përdorim (One-Time Password OTP). Kodi paraqitet me shtypjen e butonit që gjendet në TOKEN pajisjen duke paraqitur kështu algoritmin e sigurisë prej 8 numrave.

- Përmes kombinimit të TOKEN pajisjes, ID-së së shfrytëzuesit dhe parullës sekrete bëhet identifikimi i klientit në sistemin e **NLB Klik**.

- Kodi i paraqitur në TOKEN pajisje në mënyrë automatike zhduket pas 20 sekondave dhe për lidhjen e radhës në **NLB Klik** shfrytëzuesi duhet të shtyp sërish butonin për gjenerimin e kodit.

- Duhet pasur kujdes pasi që gjenerimi i kodit në TOKEN pajisje10 herë radhazi, pa e përdorur atë për tu lidhur në ueb faqe të **NLB Klik**, do të shkaktoj bllokimin e TOKEN pajisjes.

- Nëse klienti ka gabuar 5 herë radhazi në shënimin e kodit të paraqitur nga TOKEN pajisja për tu lidhur në **NLB Klik**, atëherë TOKEN pajisja del jashtë sinkronizimit. Në këtë rast klienti duhet të kontaktojë bankën për të mundësuar sinkronizimin e

TOKEN pajisjes dhe përdorimin e mëtutjeshëm të tij.

5. Informacione per tu konsideruar rreth M-TOKEN Aplikacionit

- mToken është një aplikacion që përdoret në celular për të identifikuar përdoruesit dhe për të konfirmuar transaksionin e kryer nëpërmjet shërbimit bankar E-Klik.

- mToken kryen të njëjtin funksion si tokeni fizik, dallimi është se aplikacioni i tokenit instalohet në celular, që e bën atë më të përshtatshëm dhe të lehtë për t'u përdorur.

- Kur filloni regjistrimin për të përdorur mToken në celularin tuaj, është e nevojshme që të shtypni kodin e aktivizimit. Pas kësaj, do t'ju ofrohet mundësia për të përzgjedhur dhe konfirmuar PIN-in që ju do ta përdorni sa herë që i qaseni mToken aplikacionit në celular.

- Qasja në internet është e nevojshme vetëm kur shkarkoni aplikacionin, për aktivizim (inicializimi fillestar i aplikacionit), dhe kur ndryshoni PIN-in. Pas shkarkimit dhe aktivizimit të mToken qasja në internet nuk është më e nevojshme, gjë që e bën mToken aplikacionin të disponueshëm si brenda ashtu edhe jashtë vendit. Në këtë mënyrë ju nuk duhet të shqetësoheni për shpenzimet dhe cilësinë e shërbimit të internetit.

- mToken mund të përdoret në tri gjuhë: Shqipe, Angleze, Sërbe.

- mToken ofron të njëjtin nivel të sigurisë sikurse tokeni fizik dhe është i mbrojtur edhe nga PIN-i që e din vetëm pronari. Ju mund të ndryshoni PIN-in e mToken në çdo kohë.