ТТК БАНКА АД СКОПЈЕ

ПРЕПОРАКИ ЗА БЕЗБЕДНО КОРИСТЕЊЕ НА ЕЛЕКТРОНСКИТЕ БАНКАРСКИ УСЛУГИ

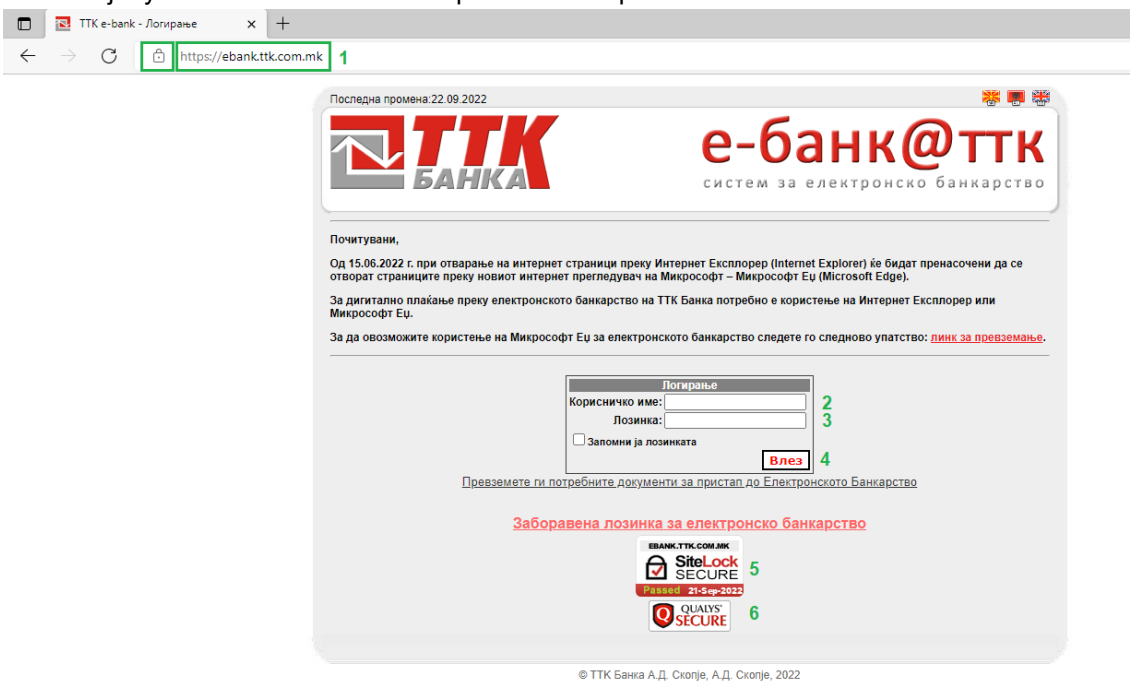
Скопје, октомври 2023

СОДРЖИНА

1. Пристап до услугите на Електронското Банкарство....3
2. Безбедносни проверки на Електронското банкарство....3
3. Идентификување на Електронското Банкарство....4
4. Безбедносни препораки за корисниците....6
   4.1 Заштита на средствата за пристап и авторизација....6
5. Најчести напади кои се случуваат и заштита од истите....6
   5.1 Кражба на идентитет (Identity Fraud)....7
   5.2 Социјален Инженеринг (Social Engineering)....7
   5.3 Напад преку посредник (Man in the middle)....7
6. Сигурност на дигиталниот сертификат....7
7. Останати сигурносни напомени....7
8. Приговор....8

1. ПРИСТАП ДО УСЛУГИТЕ НА ЕЛЕКТРОНСКОТО БАНКАРСТВО

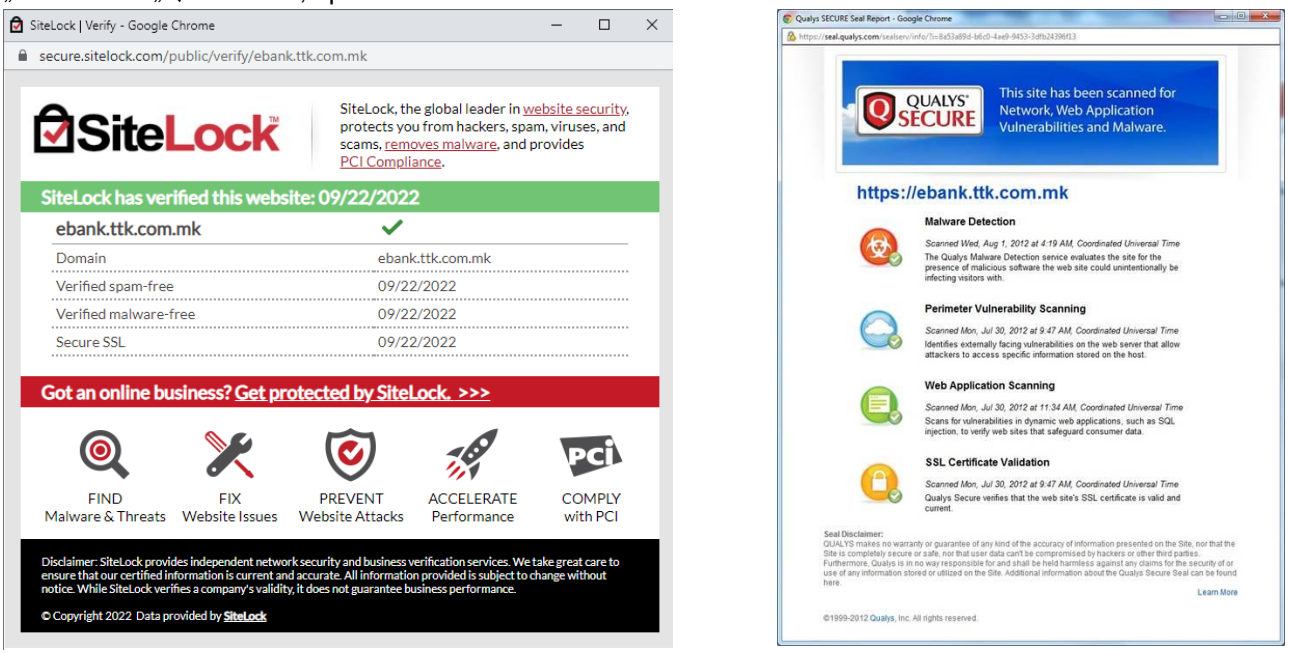
Пристапувањето до услугите на електронско банкарство на ТТК Банка АД Скопје се врши преку веб-адресата *https://ebank.ttk.com.mk* **(1)**, по што се појавува почетната страница на електронското банкарство која е прикажана на слика 1, каде се внесува корисничкото име **(2)** и лозинката **(3)** добиени од Банката. По внесувањето на корисничкото име и лозинката со кликање на копчето „*Влез*“ **(4)** корисникот се најавува на системот за електронско банкарство.



Слика 1. Почетната страница на електронското банкарство на ТТК Банка

2. БЕЗБЕДНОСНИ ПРОВЕРКИ НА ЕЛЕКТРОНСКОТО БАНКАРСТВО

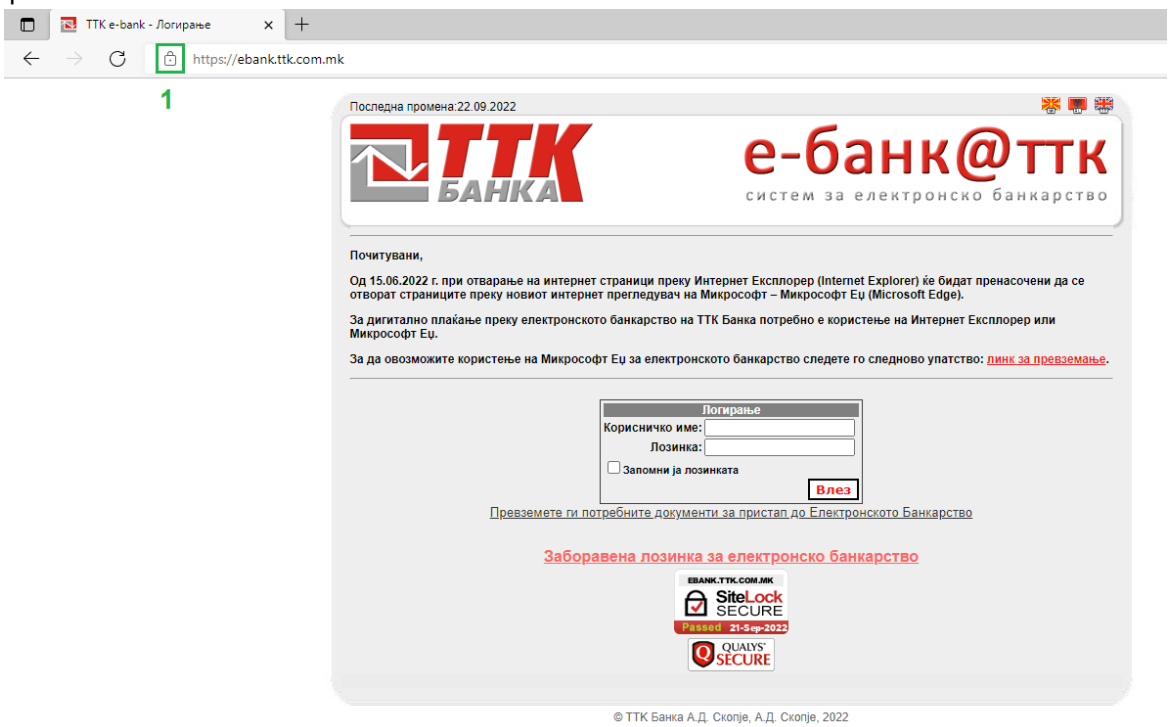
Линковите „*SiteLock*“ **(5)** и „*QUALYS®*“ *SECURE* **(6)** ги прикажуваат извештаите за безбедносните проверки кои постојано се извршуваат на страницата за електронското банкарство од страна на „*SiteLock*“ и „*QUALYS®*“, прикажани на слика 2.



Слика 2. Извештаи за безбедносните проверки на страницата за електронско банкарство

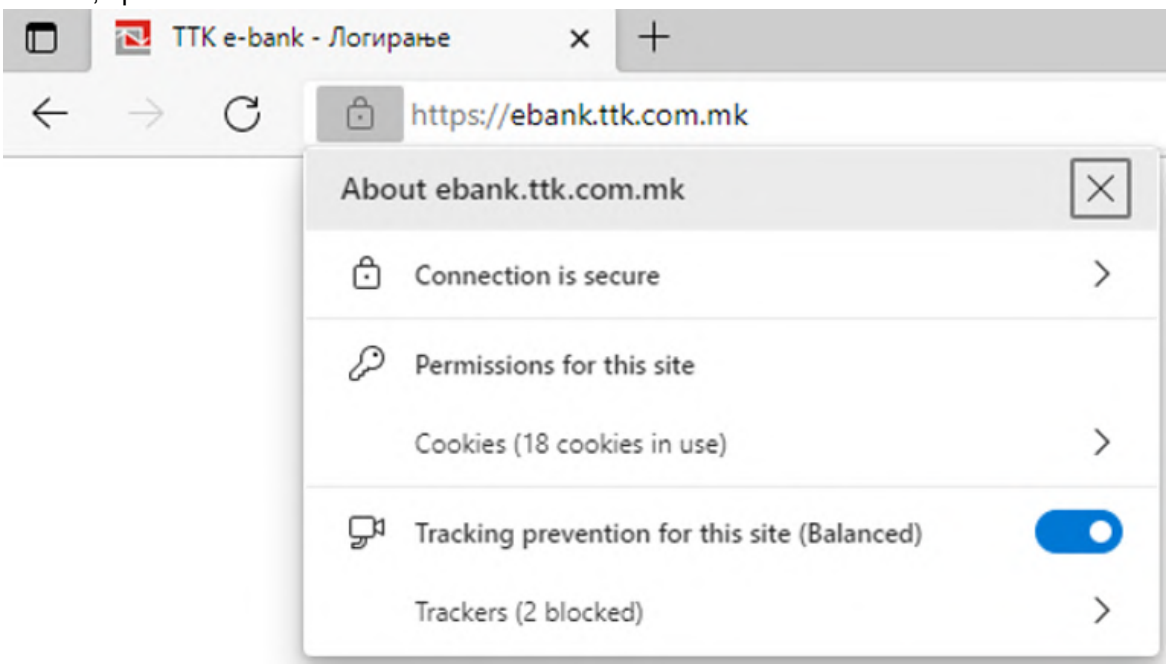
3. ИДЕНТИФИКУВАЊЕ НА ЕЛЕКТРОНСКОТО БАНКАРСТВО

Комуникацијата меѓу корисниците на електронското банкарство и Банката (https://ebank.ttk.com.mk) преку Интернет е со користење на безбедна 128 битна Transport Layer Security 1.0 енкрипција. Корисникот на електронското банкарство може да изврши проверка на автентичноста на електронското банкарство на ТТК Банка АД Скопје со кликање на иконата за безбедност **(1)** во адресната лента на пребарувачот како што е прикажано на слика 3.



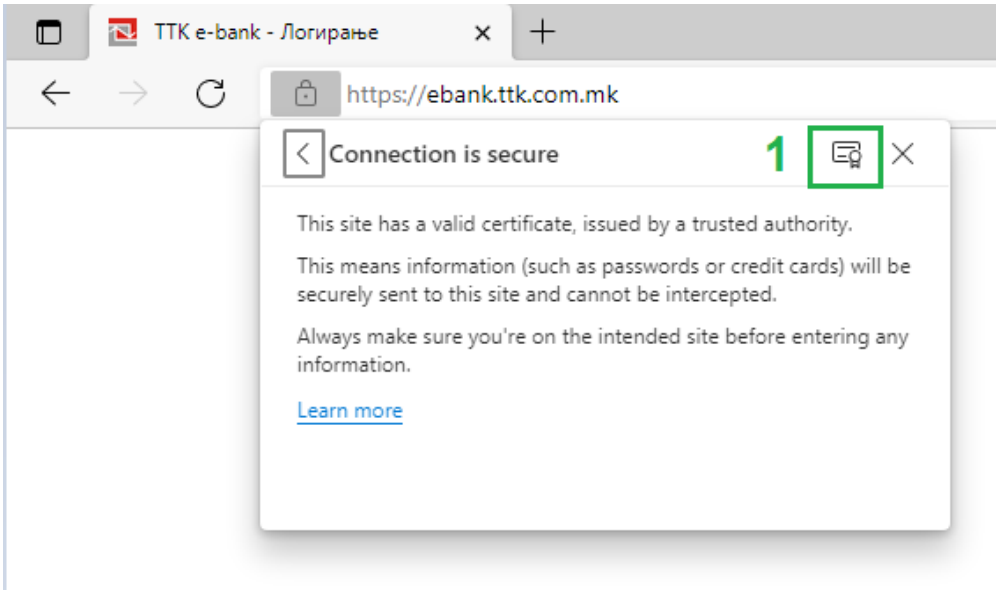
Слика 3. Приказ на иконата за безбедност во адресната лента на пребарувачот

По кликнување на иконата за безбедност ќе се појави прозорец во кој се прикажани информациите за безбедност како и опциите кои самиот корисник ги има овозможено или за кои има дадено согласност да се овозможат, прикажани на слика 4.



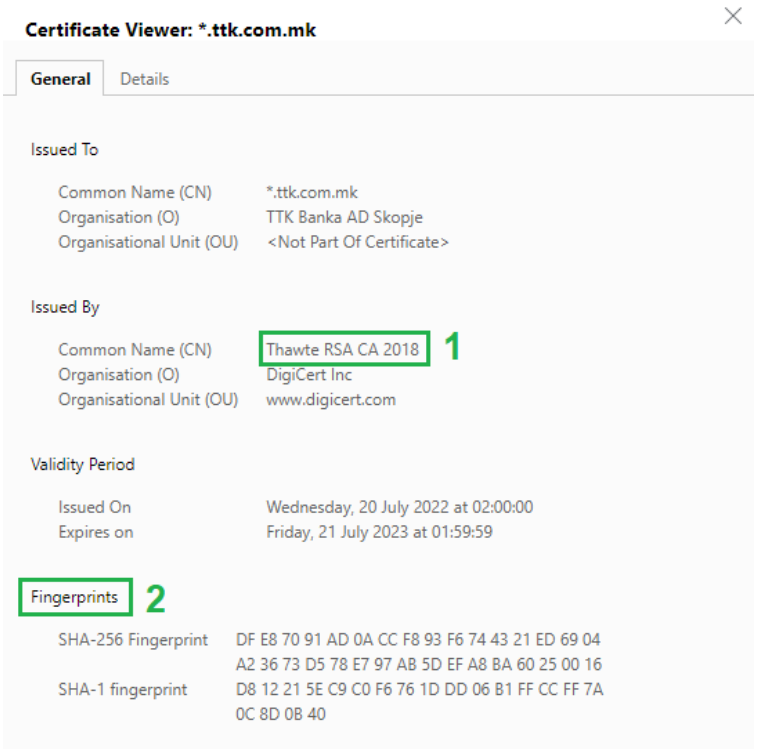
Слика 4. Информации за идентитетот на https://ebank.ttk.com.mk

За да се прегледа серверскиот сертификат за потврда на идентитетот на Банката (*https://ebank.ttk.com.mk*), треба да се избере опцијата „*Connection is secure*“ и потоа да се избере иконата за приказ на серверскиот сертификат **(1)** како што е прикажано на слика 5.



Слика 5. Приказ на иконата за приказ на серверскиот сертификат

За потврдување на автентичноста т.е. идентитетот на апликацијата за електронско банкарство (*https://ebank.ttk.com.mk*), банката користи дигитален сертификат „*Thawte RSA CA*“ **(1)** издаден од меѓународен издавач на дигитални сертификати „*Thawte*“. Исто така може да се види и провери автентичноста на серверскиот сертификат преку споредување на „*Fingerprint*“ кодот **(2)**, кој е прикажан на слика 6.



Слика 6. Податоци за серверскиот сертификат за идентификација на https://ebank.ttk.com.mk

Напомена: Thawte е меѓународно признаен авторитет за издавање на дигитални сертификати.

4. БЕЗБЕДНОСНИ ПРЕПОРАКИ ЗА КОРИСНИЦИТЕ

Со цел да се намали ризикот при сурфање на интернет препорачано е да се инсталира квалитетен автивирусен софтвер и воедно да се користи заштитната мрежа (firewall). Антивирусниот софтвер штити од инсталација на малициозен софтвер на компјутерот, го предупредува корисникот доколку сака да посети малициозна или заразена веб-страница и слично. Редовно инсталирајте ги најновите сигурносни надградби кои ги нуди производителот на оперативниот систем. Не користете застарени оперативни системи за кои производителот престанал да објавува сигурносни надградби.

Најчести човечки грешки се:

- Отворање на малициозни и сомнителни документи и слики преку електронска пошта.
- Кликнување на непознати интернет (URL) адреси.
- Испраќање лозинки или други доверливи информации до злонамерен и непознат примател.
- Трансфер на пари на неовластен (злонамерен) непознат примател и слично.

Безбедносни мерки за корисничките компјутери:

- По завршување со активностите, задолжително е потребно да се одјавите од системот за елекронско банкарство.
- За работа преку електронското банкарство корисникот треба да користи безбедни компјутери кои се одржуваат од администратори во кои корисникот има доверба.
- Не користете јавни компјутери или јавни мрежи за пристап до електронското банкарство или компјутери до кои разни лица имаат пристап.
- Се препорачува користење на легални верзии на оперативни системи и апликативен софтвер кои редовно се надградуваат со најновите верзии издадени од производителите на софтверот.
- Се препорачува користење на антивирусни пакети и постојана надградба на нивните бази.
- Не користете линкови од трети страни кои тврдат дека водат до страницата за најава во електронското банкарство.
- Се препорачува непознати/неочекувани електронски пораки да се третираат со посебно внимание и да се обрне внимание на испраќачот, воедно никогаш да не се отвараат линкови од непознати испраќачи и да не се внесуваат лични податоци.

Безбедносни мерки за корисничките мобилни уреди:

- Се препорачува мобилниот уред постојано да биде заклучен со лозинка или пин.
- Не се препорачува да пристапувате до електронското банкарство од мобилниот уред преку јавни безжични (Wi-Fi) мрежи.

4.1 ЗАШТИТА НА СРЕДСТВАТА ЗА ПРИСТАП И АВТОРИЗАЦИЈА

Средствата за пристап до електронското банкарство (*https://ebank.ttk.com.mk*) како лозинката, корисничкото име, дигитален сертификат или лозинката за дигиталниот сертификат, се во сопственост на корисникот и не треба да се споделуваат со други лица.

Доколку не се придржувате до овие препораки, може да се случи т.н. кражба на идентитетот при што потенцијалниот напаѓач кој ќе дојде до Вашите податоци за идентификација, може лажно да се претстави како Вас со што ќе му биде дозволено да пристапи до Вашите сметки и да врши трансакции без знаење на Банката. Затоа, секој обид за доаѓање до овие Ваши податоци од било кое лице, без разлика дали лично, по телефон или преку Интернет, веднаш третирајте го како обид за кражба кој треба да го пријавите во најблиската филијала или експозитура на ТТК Банка АД Скопје.

Сигурносни препораки за заштита на средствата за авторизација:

- Комбинацијата од корисничкото име и лозинката е само за корисникот и не треба да биде споделувана со други лица.
- Не се препорачува зачувување на комбинацијата од корисничкото име и лозинката во пребарувачот преку кој корисникот пристапува до почетната страница во електронското банкарство.
- Не се препорачува запишување на комбинацијата од корисничкото име и лозинка.
- Се препорачува периоднично (или по потреба) менување на лозинката.

- Се препорачува користење на сложени лозинки, составени од мала и голема буква, броеви, специјални знаци и притоа должината да биде најмалку осум карактери.
- Не се препорачува користење на една иста лозинка на повеќе сметки.
- Не се препорачува креирање на лозинка која го содржи корисничкото име, имиња на блиски личности, значајни датуми и слично.
- Се препорачува шифрата за токенот кој се користи за плаќање преку мобилното банкатство да не се споделува со други лица.

Доколку ја заборавите лозинката за влез во електронското банкарство изберете ја опцијата „*Заборавена лозинка за електронско банкарство*“ која се наоѓа под формата за најава во електроското банкарство или посетете било која од експозитурите и филијалите на ТТК Банка АД Скопје, каде со приложен документ за лична идентификација ќе Ви биде издадена нова лозинка.

5. НАЈЧЕСТИ НАПАДИ КОИ СЕ СЛУЧУВААТ И ЗАШТИТА ОД ИСТИТЕ

Нападите во дигиталниот простор (сајбер-напади) можат да предизвикаат сериозни последици, како од финансиска, така и од репутациска природа. Со цел запознавање, превентива и заштита на корисникот во продолжение се опишани најчестите сајбер напади.

5.1 КРАЖБА НА ИДЕНТИТЕТ (Identity Fraud)

Кражба и злоупотреба на идентитет претставува недозволено користење на податоци кои се стекнати на нелегален начин, но всушност се сопственост на корисникот. Овие податоци се користат за неовластено здобивање со информации или финансиски средства, предизвикување на материјална или репутациска штета и слично.

Примери за кражба и злоупотреба на идентитет во електронското банкарство:

- Нелегално здобивање и користење на средствата за пристап и работа со електронското банкарство (корисничко име и лозинка, дигитален сертификат и лозинка за дигиталниот сертификат).
- Злоупотреба на информациите за сметките и производите кои се во сопственост на корисникот, злоупотреба на личните податоци на корисникот, како и неовластено вршење на трансакции од сметките на корисникот.

5.2 СОЦИЈАЛЕН ИНЖЕНЕРИНГ (Social Engineering)

Социјалниот инжженеринг претставува обид за манипулација, со цел корисникот да открие доверливи податоци кои напаѓачот потоа може да ги искористи за свои нелегални цели. Најчесто во социјалниот инженеринг се користи лажно претставување, на пример во име на Банката, со цел корисникот да ги даде своите податоци.

Постојат различни техники на социјално инженерство, но најчесто користени се:

- Испраќање лажни e-mail пораки.
- Лажно претставување преку телефонска комуникација.

5.3 НАПАД ПРЕКУ ПОСРЕДНИК (Man in the middle)

Преку оваа техника за напад, а како резултат на претходна инфекција на пребарувачот (Web Browser) со злонамерен софтвер, корисникот се доведува во заблуда дека комуницира со официјалната страница на Банката, а всушност коминуницира со страна наменета за кражба на доверливи податоци како корисничко име, лозинка, број на кредитна картичка и слично. Затоа е многу важно корисникот да врши проверка на идентитетот на страницата до која тој пристапува.

6. СИГУРНОСТ НА ДИГИТАЛНИОТ СЕРТИФИКАТ

- Инсталирајте го дигиталниот сертификат само на компјутерите до кои имате пристап само Вие и евентуално други лица во кои имате доверба.
- При инсталацијата на дигиталниот сертификат задолжително користете високо ниво на сигурност на сертификатот (enable strong private key protection), односно при секое користење сертификатот да бара лозинка.
- Лозинката на дигиталниот сертификат, исто како и лозинката за најава на електронското банкарство не треба да ја споделувате со други лица или да ја запишувате на места до кои неовластени лица може да добијат пристап.
- Не го инсталирајте дигиталниот сертификат на јавни компјутери и не ја препраќајте електронската

пошта со дигиталниот сертификат на други лица.
- Доколку се сомневате дека дигиталниот сертификат е компромитиран, веднаш побарајте од Банката негово блокирање.

7. ОСТАНАТИ СИГУРНОСНИ НАПОМЕНИ

- Банката на ниту еден начин (преку телефон, електронска пошта или форма различна од формата за најава на електронското банкарство) нема да Ви ги побара средствата за пристап и авторизација во електронското банкарство, но доколку некој Ви ги побара овие информации на било кој начин, тогаш веројатно претставува обид за кражба на податоци и случајот веднаш треба да биде пријавен во Банката.
- По најавата, во електронското банкарство стои податок за последна најава. Доколку овој податок не соодветствува со датумот и времето на Вашата последна најава, задолжително известете ја Банката и извршете промена на лозинката.
- Вршете редовна проверка на состојбата и трансакциите на Вашите сметки во Банката и доколку забележите одредени нелогичности, веднаш известете ја Банката.
- Користењето на сервисот за електронско банкарство не зависи од бројот на вашата платежна картичка, ниту пак од пинот на платежната картичка.
- Доколку добиете некоја сомнителна електронска порака или телефонски повик веднаш известете ја Банката со повикување на телефонскиот број на Банката (02/3247000 лок. 020) или со испраќање на електронска порака на електронската пошта на Банката (it@ttk.com.mk), исто така може да посетите некоја од експозитурите и филијалите на ТТК Банка АД Скопје.
- Согласно Законот за заштита на личните податоци и интерните акти на Банката, без Ваша писмена согласност ниту еден Ваш личен податок како што е телефонски број, електронска пошта или домашна адреса не смее да биде дадена на трето лице (агенција, друга компанија и слично).

8. ПРИГОВОР

Доколку корисникот има приговор, потреба од обезбедување корисничка поддршка, пријава или сомневање за сомнителни и/или изменети трансакции, пријава за сомнителна работа на софтверското решение, пријава на аномалии во текот на користење на услугите на современите канали и/или пријава за можни обиди за социјален инженеринг на страницата, корисникот може да поднесе пријава на електронската пошта на Банката (it@ttk.com.mk), на телефонскиот број на Банката (02/3247000 лок. 020) или во најблиската филијала или експозитура на ТТК Банка АД Скопје.