ПРЕПОРАКИ ЗА БЕЗБЕДНОСТ – OBSGN@t и „Moja Banka“

Најдобри практики

ИТ безбедноста вклучува усвојување на одредени техники и најдобри практики за заштита на вашите компјутери и вашите интереси кога користите ИТ-ресурси, какви што се онлајн банкарските услуги на Охридска банка. Овие техники и најдобри практики се развиени од страна на специјалисти за ИТ-безбедност, а вие е важно да знаете да ги применувате наједноставните од нив.

- **Заштитете си ја лозинката**

Вашата лозинка обезбедува важна заштита за да се гарантира дека онлајн трансакциите можете да ги извршувате во целосна безбедност. Меѓутоа, за да се обезбеди оптимална заштита, лозинката треба да ги задоволи долунаведените најдобри практики.

- Избор на лозинка: изборот на „силна“ лозинка ве заштитува од кражба на идентитетот. Вашата лозинка не треба да биде тривијална (да не ги повторува истите знаци или низи од знаци) и треба да биде тешка за погодување (на пример, не треба да биде денот на вашето раѓање).
- Користење на лозинка: внесувајте ја лозинката само на безбедната најавна страница на OBSGNet, на адресата https://www.obsgnet.com.mk.

Не ја откривајте Вашата лозинка на никого.
Охридска банка никогаш нема да ве праша која ви е лозинката.

- **Одјавете се откако ќе завршите со работењето на страната за електронско банкарство:**

Откако ќе се најавите на системот за електронско банкарство, се отвора една сесија за разгледување на вашите податоци. Додека е отворена оваа сесија, можете да се движите од страница на страница и да вршите одредени операции без да морате повторно да се идентификувате. Иако оваа можност е практична, таа може да му дозволи некому да го искористи вашиот компјутер за да ја прелиста вашата сметка и да изврши некои операции без ваше знаење.

Откако ќе завршите со разгледувањето на вашите сметки, од витална важност е да се одјавите користејќи го копчето „Одјава“. Не е доволно само да ја затворите страницата на прелистувачот. Запомнете дека Охридска банка нема да може да отфрли ниедна трансакција што е извршена во текот на сесија отворена на ваше име.

- **Деактивирајте ја функцијата за автоматско пополнување (AutoComplete) на вашиот прелистувач:**

Повеќето веб-прелистувачи ви нудат да ги зачуваат корисничките имиња и лозинките што ги користите во формуларите за најава, вклучително и деталите за вашата најава на онлајн банкарството. Функцијата за автоматско пополнување ви дозволува да пристапите до вашата сметка во некој подоцнежен момент без да морате повторно да го внесете вашето корисничко име. Иако ова е практично, функцијата за автоматско пополнување би можела да му помогне на некое лице или на некој злонамерен софтвер да го искористи вашиот компјутер за да пристапи до вашата сметка без ваше знаење.

OHRIDSKA BANKA

Од витална важност е да ја деактивирате функцијата за автоматско пополнување на вашиот прелистувач.
Запомнете дека Охридска банка нема да може да отфрли ниедна трансакција што е извршена во текот на сесија отворена на ваше име.

- **Обезбедете го вашиот компјутер:**

Пред да започнете со прелистување на интернет, треба да го заштитите вашиот компјутер од потенцијални злонамерни напади. За да го направите тоа, следете ги упатствата наведени подолу:

- Ажурирајте го вашиот оперативен систем и софтвер: за да го заштитите вашиот компјутер од злонамерни напади, од витална важност е да ги одржувате вашиот оперативен систем и вашиот софтвер во ажурирана состојба. Затворањето на познатите безбедносни пропусти ги прави неефективни највообичаените методи за напад.
- Инсталирајте антивирусен софтвер: на вашиот компјутер треба да инсталирате антивирусен софтвер дури и кога тој софтвер е бесплатен. Таквиот софтвер ве заштитува со тоа што ги идентификува и ги блокира злонамерните апликации инсталирани на вашиот компјутер. Антивирусниот софтвер ја проверува и веродостојноста на датотеките што ги преземате од интернет или што ги примате преку електронска пошта. Исто така, треба да се погрижите вашиот антивирусен софтвер да биде во ажурирана состојба.

** најважните програми што треба да се ажурираат се оние кои пристапуваат до интернет (прелистувач, електронска пошта итн.) и познатите софтверски пакети (Office pack, Adobe suite, Java, итн.)*

- **Проверете ја веродостојноста на веб сајтот на кој сте приклучени:**

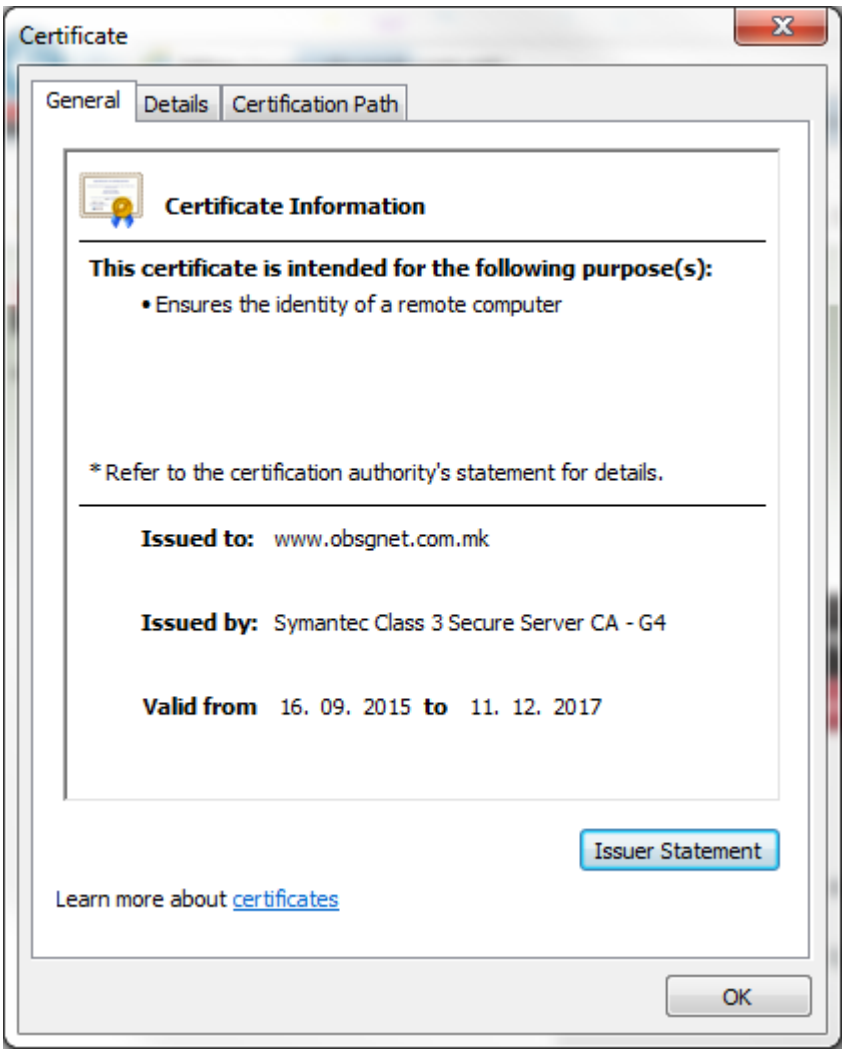
Без разлика на тоа дали сте на некој банкарски веб сајт или на некој веб сајт за електронска трговија, пред да ги внесете вашите податоци за најава или пред да извршите каква било трансакција, важно е да се уверите дека веб сајтот е официјален и безбеден. Следете ги овие упатства за да ја проверите веродостојноста на веб сајтот на кој сте приклучени:

- Проверете го идентификаторот URL на веб сајтот во полето за веб-адресата: URL е уникатниот идентификатор за веб-страницата на којашто сте приклучени и може да се види во полето за веб-адресата на вашиот прелистувач. Со внимателна проверка на оваа страница, можете да видите дали веб сајтот на којшто сте приклучени е лажен, зашто неговата адреса во тој случај ќе мора да биде различна од онаа на официјалниот веб сајт (на пр. www.particulier.sg.fr, наместо www.particuliers.societegenerale.fr).

- Проверете го префиксот на адресата: секоја официјална интернет-локација за електронско банкарство или електронска трговија користи безбедни комуникациски протоколи со своите клиенти. Ако сте на безбеден вебсајт, пред URL ќе стојат буквите „https“ (наместо „http“).

Целосната адреса на безбедната локација на Охридска банка е:
https://www.obsgnet.com.mk

- Проверете го безбедносниот сертификат: сертификатот се користи за да обезбеди гаранција дека вебсајтот ѝ припаѓа на Охридска банка (www.obsgnet.com.mk). Вашиот веб-прелистувач може да го прикаже безбедносниот сертификат што го користи страницата на која што се наоѓате. Сертификатот треба да изгледа вака:



- **Специфични заштитни мерки за паметни телефони:**

Сè поголемата употреба на паметните телефони и сè поголемиот развој на банкарските услуги за ваквите уреди доведува до појава на нови безбедносни ризици. Честопати се смета дека паметните телефони се слични на мобилните телефони, но во реалноста тие едноставно се компјутери што може да се користат за телефонирање. Според тоа, безбедносните мерки, применливи за еден компјутер (видете погоре), се подеднакво валидни и за еден паметен телефон.

Меѓутоа, паметните телефони бараат и дополнителни специфични заштитни мерки:
Заштитете го вашиот телефон со (нетривијална) лозинка и нагодете вашиот екран автоматски да се заклучува кога не се користи.

- Погрижете се да ги применувате сите ажурирања препорачани од вашиот системски провајдер
- Преземајте апликации само од официјални продавници за апликации (на пр. Apple Store, Google Play Store). Во спротивно, ризикувате на вашиот паметен телефон да преземете злонамерни апликации
- Не отклучувајте го никогаш оперативниот систем на вашиот паметен телефон (на пр. jailbreak, rooting), зашто со тоа се наголемува вашата изложеност на ризици
- Не складирајте никакви декриптирани доверливи податоци на вашиот паметен телефон
- Инсталирајте антивирусен софтвер и одржувајте го во ажурирана состојба

Запомнете дека е од витална важност да <u>се преземаат истите мерки на претпазливост со паметен телефон како оние што се преземаат со компјутер кога се пребарува по интернет</u>

Безбедносни мерки

Охридска Банка е свесна за безбедносните ризици што произлегуваат од осетливоста на една онлајн банкарска услуга и имплементира најсовремени безбедносни мерки за да ви обезбеди највисоко можно ниво на безбедност.

- **Механизми и процедури за автентикација:**

Автентикацијата е клучен елемент на безбедноста на онлајн банкарската услуга. Оваа процедура, која ви дава пристап до вашите сметки за да ги разгледувате и за со нив да управувате, ѝ дозволува на Охридска банка формално да ве идентификира.

Елементите што се користат за автентикација се вашето корисничко име и лозинката. Вашето корисничко име е уникатно и ви се доделува кога ќе се регистрирате за онлајн услугите. Кога ќе се регистрирате за онлајн услугите, вам ви се доделува една однапред зададена лозинка, а потоа ви се прикажува онлајн формулар во кој треба да ја смените вашата лозинка откако првпат ќе се најавите.

<u>Автентикација со лозинка</u>

Новата лозинка, која треба да ги задоволува препораките во делот „Најдобри практики: заштитете си ја лозинката“, може да се смени во секое време на следнава адреса: https://www.obsgnet.com.mk/Retail/Account/ForgotPassword. Вашето корисничко име и вашата лозинка ги користите за да пристапите до вашите сметки.

Никогаш не откривајте му ја вашата лозинка никому.
Запомнете дека <u>Охридска банка никогаш нема да ве праша која ви е лозинката</u>

Автентикација преку OTP

OTP-калкулаторот генерира нова лозинка за еднократна употреба секогаш кога ќе се најавите, во комбинација со Вашето корисничко име и вашата лозинка кои ги користите за да пристапите до вашите сметки.

Потврда преку OTP

Покрај тоа, може да биде неопходно да се изврши дополнителна операција на автентикација за да се завршат одредени трансакции, со цел да се потврдат вашиот идентитет, вашата согласност и валидноста на трансакцијата. Охридска банка користи решение со еднократна лозинка (One-Time Password, OTP).

Калкулаторот ја генерира еднократната лозинка, којашто морате да ја внесете на вебсајтот за да ја потврдите трансакцијата.

Автентикација преку m-Token

За автентикација со m-Token, треба да ги внесете вашето корисничко име и лозинката и да ја внесете генерираната нова OTP-лозинка од апликацијата m-Token секој пат кога ќе се најавите.

Потврда преку m-Token

Покрај тоа, може да биде потребно да се изврши дополнителна автентикација за да се завршат одредени трансакции, со цел да се потврдат вашиот идентитет, вашата согласност и валидноста на трансакцијата.

За таа цел, вебсајтот за електронско банкарство ќе прикаже QR-код кој треба да биде скениран од апликацијата m-Token на вашиот паметен телефон. Износот на плаќањето и сметката на примачот кои се читаат од QR-кодот потоа ќе бидат искористени за генерирање на еднократна лозинка (OTP) што може да се употреби само со токму таа трансакција.

За да ја потврдите трансакцијата, во апликацијата за електронско банкарство треба да ја внесете генерираната OTP-лозинка.

- **Шифрирање (енкрипција) на комуникациите:**

Онлајн банкарската услуга го користи шифрираниот комуникациски протокол SSLv3/TLS (Secure Socket Layer version 3 / Transport Layer Security). Активирањето на шифрирањето ја зајакнува HTTP-комуникацијата, којашто консеквентно се преименува во HTTPS (каде што S стои за „сигурност“). HTTPS-протоколот гарантира дека сите информации што се разменуваат на вебсајтот се безбедни и доверливи.

Секогаш можете да проверите дали локацијата на којашто сте приклучени е безбедна:

- на адресата на вебсајтот ќе ѝ претходи префиксот „https“
- кај некои прелистувачи, во полето за статусот ќе биде прикажано и лого на катинар

Сертификат за проширена валидација (Extended Validation Certificate, EV)

- Во некои прелистувачи, полето за адресата ќе стане зелено и ќе прикажува лого на сертификација

Целосната адреса на безбедната локација на Охридска Банка е:
https://www.obsgnet.com.mk

- **Процедура за автоматска одјава:**

Заради ваша безбедност, по изминати 30 минути ќе бидете автоматски одјавени од услугата. Ова значи дека ако сте го напуштиле компјутерот без да се одјавите, никој не ќе може да го користи вебсајтот место вас. За повторно да се најавите, морате повторно да ги внесете вашето корисничко име и лозинката.

Од витална важност е да се одјавите со користење на копчето „Одјава“ откако ќе завршите со разгледувањето на вашите сметки. Запомнете дека Охридска банка нема да може да отфрли ниедна трансакција што е извршена во текот на сесија отворена на ваше име.

- **Следење и архивирање:**

Заради безбедносни причини, активноста на вашиот банкарски вебсајт се следи и се архивира 24/7, во согласност со банкарските прописи што се во сила и во согласност со релевантните закони за заштита на податоци.

Каква било аномалија, што ќе се детектира, ќе покрене една длабинска анализа, како и ад хок процедури за да се обезбеди сигурното функционирање и континуитетот на услугата во секое време.