E-banking сигурносни препораки за корисниците

Како дел од постојаната грижа кон корисниците, Стопанска банка АД – Скопје препорачува на своите корисници да ги примени барем следниве сигурносни мерки при користењето на E-banking сервисот на банката.

Изберете сложена лозинка

- Сложената лозинка се состои од најмалку осум знаци и содржи големи букви, мали букви и броеви. Изберете сложена лозинката за влез во E-banking системот. Што посложена лозинка толку потешко е да се погоди или пробие истата. Не користете иста лозинка за најава во E-banking системот и за најава во други системи како што се приватна е-пошта и др. Менувајте ги лозинките повремено, на пример на секои шест месеци. Не ја делете или кажувајте вашата лозинка никому.

Инсталирајте сигурносен софтвер/пакет

- Постојат многу злонамерни софтверски решенија чија единствена цел е да го надгледуваат користењето на тастатурата и периодични да „звонат дома“ со резултатите од надгледувањето. Овие типови на вируси се наречени „надгледувачи на тастатурата“ чија цел е да ја откријат вашата лозинка. За да се намали ризикот од крадење на вашата лозинка од страна на вируси, инсталирајте софтвер за Интернет заштита кој обезбедува комплетна заштита од вируси и крадење на лозинки. Изберете софтверско решение препорачано од повеќе доверливи и независни извори. Софтверските решенија/Пакети за Интернет заштита може да вклучуваат но не се ограничени на: антивирусно решение, огнен ѕид, протившпионска заштита, заштита на кражба на идентитетот.

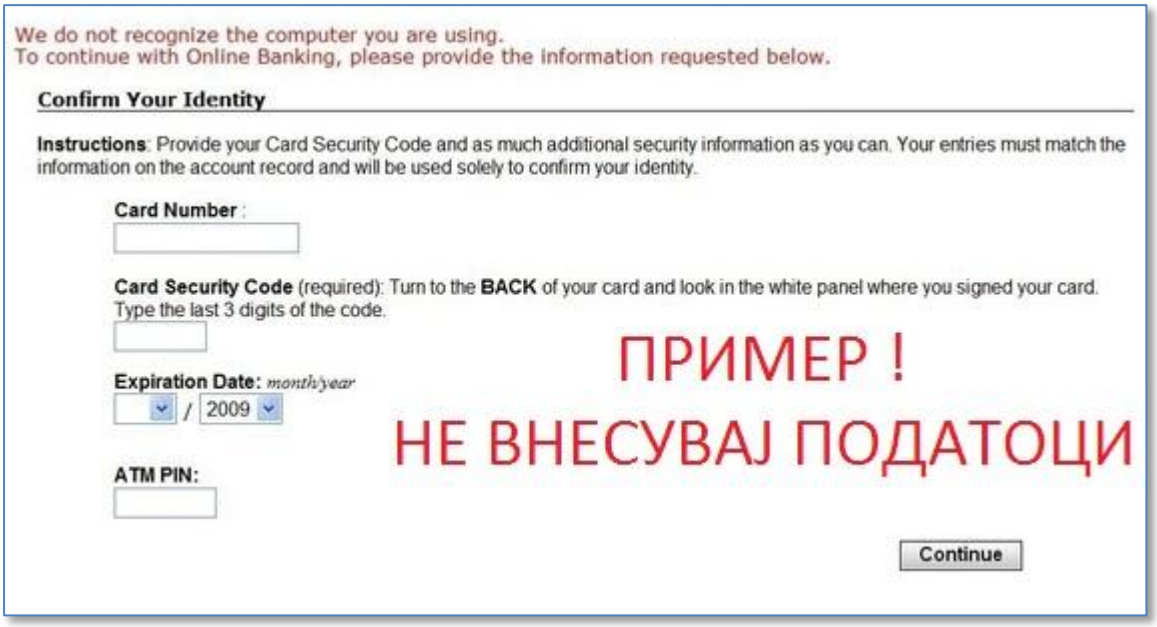
Не кликајте на линковите за врска во е-поштата

- Банката или нејзините вработени никогаш нема да ве прашаат за вашата лозинка за влез во E-banking системот. Доколку добиете е-пошта во која се бара вашата лозинка и/или корисничко име, тоа е само обид некој да ја дознае вашата лозинка/корисничко име. Не кликајте на линковите во е-поштата, а пораката избришете ја веднаш. Банката може единствено да го побара вашето корисничко име, но не и лозинката, со цел да се потврди вашиот идентитет во постапка на заборавена лозинка иницирана од ваша страна.

Форми и начини за крадење на банкарски информации

- Zeus, исто така познат и како Zbot, WSNPOEM, NTOS и PRG, е најраспростанетото злонамерно софтверско решение кои криминалните поединци и/или групи го користат за крадење на банкарски информации. Овој злонамерен софтвер го заразува вашиот личен компјутер, при што од вас бара лични податоци како што се: Број на платежна картичка, ПИН код, датум на истекување на картичката и слични податоци.
- **Важно: Не внесувајте ваши лични податоци или други банкарски односно финансиски податоци. Веднаш побарајте совет од банката за следните чекори.**

- Пример за можен изглед на споменатото злонамерно софтверско решение за крадење на вашите лични и банкарски информации



- **Важно: При користење на E-banking сервисот, Стопанска банка АД – Скопје никогаш нема да ви побара да внесете Број на платежна картичка, ПИН или други лични податоци затоа што:**
  - Користењето на E-banking сервисот не зависи од бројот на вашата платежна картичка а особено не од ПИН кодот кој треба само вие да го знаете.
  - Користењето на E-banking сервисот е воспоставен со вас во строго контролирана постапка во која вие се здобивате со корисничко име од страна на Банката а лозинката по првата најава ја бирате само вие, и само вие ја знаете истата.

Користење на безжичен интернет пристап, јавни компјутери

- Избегнувајте користење на E-banking сервисот на банката преку слободен безжичен интернет пристап каков што може да се сретне по аеродромите, трговските центри или ресторанте, сем ако даденият безжичен интернет пристап не е обезбеден со Wi-Fi Protected Access (WPA) или WPA2. Останатите шеми за шифрирање како што е Wired Equivalent Privacy (WEP) лесно може да се дешифрираат со соодветен софтер, а со тоа да се дознаат вашите сензитивни информации.
- Не пристапувајте до E-banking сервисот на банката од јавен компјутер или од т.н. Интернет-Кафе. Наместо тоа користете еден компјутер/преносен компјутер.

Пратете ги вашите сметки и историјатот на трансакциите

- Внимавајте на вашите сметки и историјатот на трансакциите при користење на E-banking сервисот. Доколку видите трансакција за која се сомневате дека не сте ја одобриле, дури и да е мала по сума, контактирајте го веднаш нашиот 24 часовен инфо центар (02) 3100 109

Одјавете се по завршување на потребата од E-banking сервисот

- Доколку некој има физички пристап до компјутерот од кој го користите E-banking сервисот, секогаш одјавете се по завршување на потребата од истиот. Овој чекор ја намалува можноста некој друг физички да пристапи до компјутерот и истиот да го искористи додека вашата сесија со E-banking сервисот е сеуште активна. Најсигурен начин за комплетно одјавување е да го затворите интернет пребарувачот по завршување на потребата од E-banking сервисот.

Претпазливост за сигурност во секое време

- Сигурноста нека остане ваш врвен приоритет при користењето на E-banking сервисот. Секое лажно чувство на сигурност е само придобивка за злонамерните.