

ПРЕПОРЪКИ ЗА СИГУРНОСТ НА „ИНТЕРНЕТ БАНКИРАНЕ“ НА ТОКУДА БАНК АД

При използване на системата „Интернет банкиране“ Токуда Банк АД осигурява максимална защита на клиентските данни и на всички транзакции чрез прилагане на следните средства:

I. Защита на връзката.

Достъпът до сървърите на „Интернет банкирането“ се осъществява по криптиран https протокол. Токуда Банк АД използва сървърен сертификат, издаден от компанията Thawte, който гарантира идентичността на сървъра, към който клиентите осъществяват връзка.

II. Подписване и изпращане на транзакции чрез ТАН, изпращан по sms.

„ТАН-Транзакционен Авторизационен Номер“ /ТАН/ е уникален, еднократно използваем 6-разряден цифров код, представляващ парола за идентификация, получена по sms. Изпратеният ТАН по sms е валиден за ограничен период от време (20 минути) и може да бъде използван само веднъж. С един ТАН може да бъде подписан и/или изпратен към Банката един или пакет от електронни документи. Въвеждането по електронен път на ТАН по sms има силата на правно валиден подпис. Плащания и/или подписвания с ТАН по sms могат да правят само потребители, които са упълномощени да се разпореждат със сметките на клиента и имат регистриран телефонен номер в системата на Банката. Всеки потребител сам носи лична отговорност за опазване на получен от него ТАН.

III. Потребителско име и парола.

Всеки потребител на системата има уникално потребителско име и парола, известни само на него. При първи вход в системата потребителската парола задължително трябва да се смени.

Токуда Банк АД използва професионално средства за опазване на сигурността на компютърната си мрежа. Независимо от това, при работа със системата за „Интернет банкиране“ са много важни и предпазните мерки, предприети от Ваша страна, за защита на Вашите компютри и компютърни мрежи. Във връзка с това ние Ви предлагаме да спазвате нашите **препоръчителни мерки за сигурност**, както следва:

- A. Пазете своето потребителско име и парола, никога не го записвайте на хартия, материален носител, не го включвайте в електронни съобщения и не ги давайте на никого – те са лични!
- B. Използвайте сигурни пароли – съдържащи малки и големи букви, препинателни знаци и цифри (a-z, A-Z, 0-9, !?+”%=:/_№@#\$\$%^&*()_+), съдържащи най-малко седем символа и не основани на лична информация, фамилни имена, адреси и други. Периодично променяйте паролата си за достъп (например на всеки 1-3 месеца).
- C. За достъп в системата винаги изписвайте в полето за въвеждане на адрес <https://rbank.tokudabank.bg/oraweb>. Проверете комуникационния протокол и се уверете, че <https://rbank.tokudabank.bg> има сървърен сертификат, издаден от Thawte.
- D. Не използвайте опциите за автоматично запамяване на потребителски имена и пароли!
- E. Винаги използвайте бутона “Изход”, когато приключите с работата си с „Интернет банкирането“, а не просто да затворите прозореца на брауъра, за да сте сигурни, че защитената връзка, която е била създадена с логването Ви в „Интернет банкирането“ Ви, е прекъсната.
- F. Използвайте само легални програми, закупени от доставчици, на които имате доверие. Актуализирайте ги редовно!
- G. Препоръчваме Ви да използвате програми за антивирусна защита, които са редовно поддържани и обновявани.
- H. Препоръчваме Ви да не използвате системата за „Интернет банкиране“ от компютри с неурегулиран достъп и/или в присъствието на други лица (компютърни зали, библиотеки, на компютри, използвани от други хора, освен Вас и други).