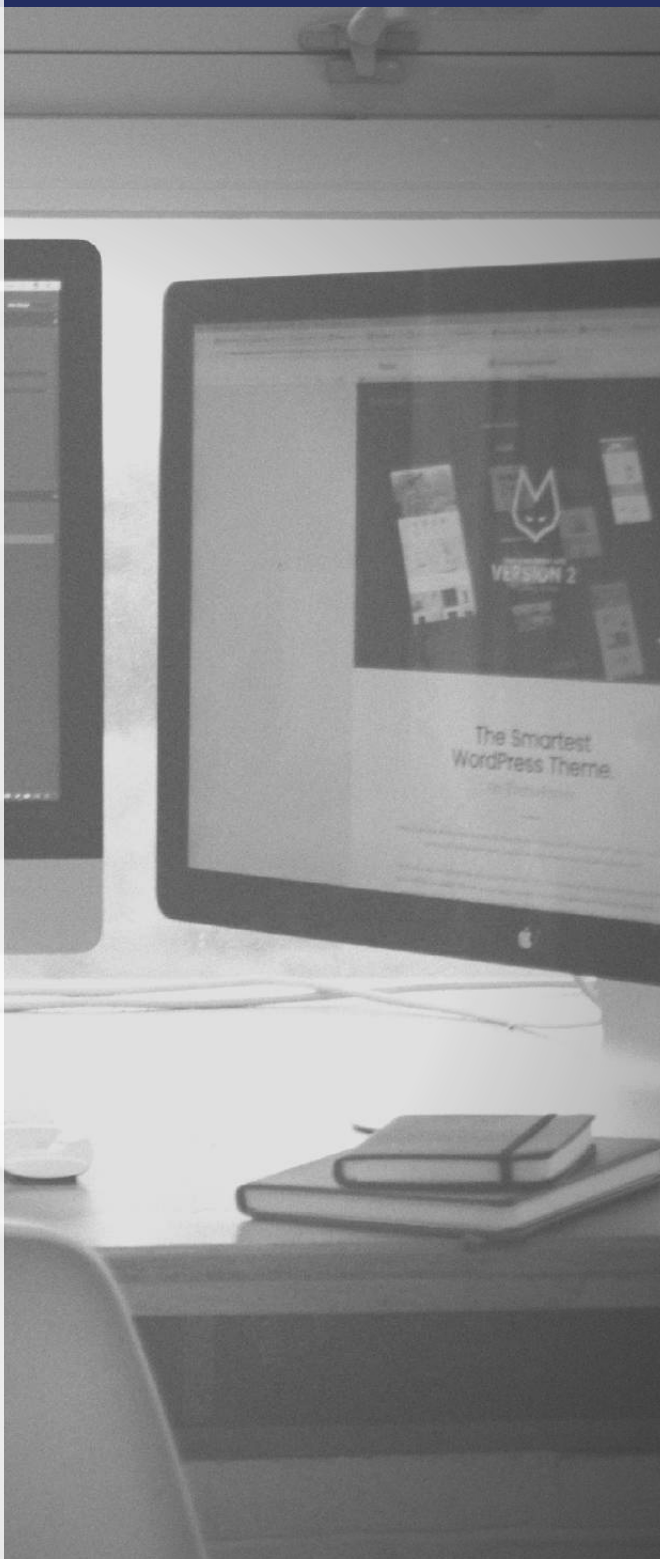
ҚАУІПСІЗДІК ТУРАЛЫ ҰМЫТПАҢЫЗ!

Eurasian Bank

Құрметті клиенттер!

Киберқылмыскерлердің құрбаны атану қауіпінің өсуіне байланысты қашықтықтан банктік қызмет көрсету (бұдан әрі - ҚБҚ) жүйесімен жұмыс істеу кезінде келесі ережелерді сақтауыңызды сұраймыз



- ҚБҚ жүйесіне кіру үшін құпия сөзді компьютердегі интернет-браузерде және тексті файлдарда немесе басқа электронды ақпарат тасымалдауыштарда сақтамаңыз.
- ҚБҚ жүйесінен өзініңіздің құпия сөзіңізді үшінші тұлғаға, оның ішінде банктің қызметкерлеріне бермеңіз.
- ҚБҚ жүйесінің веб-сайтына баннерлік сілтемелер немесе электронды поштадағы сілтемелер арқылы кіруден аулақ болыңыз.
- ҚБҚ жүйесінің ресми сайтымен қорғалған SSL-қосылудың бар-жоғын тексеріңіз.
- Жүйені пайдалану сеансы кезінде басқа веб-сайттарды пайдаланудан аулақ болыңыз.
- ҚБҚ жүйесінде жұмысыңызды аяқтағаннан кейін сессияны да аяқтауды ұмытпаңыз.
- ҚБҚ жүйесін көпшілікке қол жетімді интернетке кіру орындары және қонақ жұмыс орындары (мысалы, интернет-кафе) арқылы пайдаланудан аулақ болыңыз.
- Ұялы құрылғылардан оқшаулауды алу үшін құпия сөзді, графикалық кілтті немесе биометрикалық сәйкестендіруді пайдаланыңыз.
- Егер сіз банктен SMS-хабарландыруларды алу үшін пайдаланылып жүрген ұялы құрылғыны жоғалтсаңыз немесе сіздің SIM-картаңыз кенеттен жұмыс істемей қалса, дереу банкпен хабарласыңыз және пайдаланып жүрген SIM-картаны оқшаулау үшін өзіңіздің ұялы байланыс операторыңызға хабарласыңыз.
- ҚБҚ жүйесінде рұқсат етілмеген транзакциялардың жасалғаны жайлы банкке хабарлаңыз. Мысалы, егер сіз өзіңіз жасамаған операция бойынша SMS-хабарландыру алсаңыз. Осындай жағдайларда бірден банкке жолығу қажет.
- Өзіңіздің компьютеріңізде әкімгер өкілеттігі бар тіркеулік жазбасында тұрақты жұмыс істеуден аулақ болыңыз.
- Тексерілмеген көздерден алынған бағдарламаларды қоспаңыз (олардың ішінде ең қауіптілері электронды пошта және интернет арқылы алынған бағдарламалар болып табылады).
- Күмән тудыратын сайттарға кірмеңіз және сол сияқты электронды хаттарды ашпаңыз.
- Лицензиялық бағдарламалық қамтамасыз етуді пайдаланыңыз және операциялық жүйе үшін сындарлы жаңартуларды уақытылы орнатыңыз.
- Антивирустық сигнатураларды күнделікті жаңартып отырыңыз және жұмыс стансаңызды вирустық белсенділіктің бар-жоғын анықтау үшін тұрақты түрде толық тексеруден өткізіп тұрыңыз.
- Қауіпсіздікті арттырудың қосымша құрылғыларын (желі аралық экрандарды, тыңшы компоненттерді іздеу бағдарламаларын және т.б. құрылғыларды) пайдаланыңыз.
- Жұмыс стансасына және басқа құрылғыларға үшінші тұлғалар үшін қолжетімділікті шектеңіз.