Шановний клієнт!

З метою мінімізації ризиків, пов‘язаних з шахрайськими діями з використанням Системи дистанційного банківського обслуговування (далі - Система), банком розроблені наступні прості вимоги інформаційної безпеки, яких слід дотримуватися при використанні Системи.

1. Ніколи і ні за яких обставин не розголошуйте дані, що використовуються Вами для роботи в Системі (логін і пароль для входу в Систему, пароль до електронно-цифрового підпису, одноразовий пароль, який відправляється СМС-повідомленням і т.п.) стороннім особам, навіть отримавши лист або дзвінок від осіб, що представляються співробітниками банку і не використовуйте їх для інших систем і ресурсів в Інтернет.
2. Використовуйте Систему тільки на довірених пристроях, не використовуйте для доступу до Системи комп'ютери, встановлені в публічних місцях, чужі комп'ютери, ноутбуки, смартфони і т.п.
3. Не зберігайте логін і пароль для входу в Систему, пароль до електронно-цифрового підпису (ЕЦП) на жорсткому диску комп'ютера, а також в будь-якому іншому місці, яке може бути доступним стороннім особам.
4. Зберігайте ключі ЕЦП тільки на змінних носіях, забезпечуйте їх збереження і не записуйте на змінні носії з ключем ЕЦП іншу інформацію.
5. При використанні декількох Систем від різних банків, зберігайте ключі ЕЦП від кожної Системи на окремому носії.
6. Змінні носії з ключами ЕЦП використовуйте тільки при здійсненні переказу коштів. Відразу після проведення операцій з використанням ЕЦП відключайте носій ЕЦП від комп'ютера.
7. Змінні носії, на яких зберігаються ключі ЕЦП рекомендується шифрувати.
8. У разі компрометації або підозри на компрометацію ЕЦП, необхідно терміново повідомити банк для блокування ключів ЕЦП, провести процедуру генерування і реєстрації нових ключів ЕЦП в Системі з наданням в банк оригіналів сертифікатів ЕЦП, завірених підписом Клієнта.
9. Утримуйтеся від використання комп'ютера, який використовується для роботи з Системою для розваг та інших не пов'язаних з роботою в Системі дій, в тому числі, в мережі Інтернет, а також обмежте до нього фізичний і мережевий доступ сторонніх осіб. Для запобігання зовнішніх вторгнень і виключення можливості зовнішнього підключення зловмисників до комп'ютера, який використовується для роботи з Системою, обов'язково включайте на ньому міжмережевий екран (firewall).
10. На комп'ютері, який використовується для роботи з Системою, повинна бути встановлена антивірусна програма з регулярністю оновлення вірусних баз не рідше 1 разу на день і періодичним проведенням перевірок комп'ютера на наявність шкідливого, зловмисного програмного забезпечення. Обов'язковою є регулярне оновлення операційної системи (в першу чергу це стосується оновлень безпеки).
11. У разі виявлення будь-якого шкідливого, зловмисного програмного забезпечення (віруси, троянські програми і т.д.) на комп'ютері, з якого здійснювався вхід в

Систему, необхідно обов'язково здійснити вхід в Систему з гарантовано не зараженого комп'ютера і замінити пароль доступу до Системи.

12. При створенні пароля рекомендується використовувати комбінації з букв, цифр і спеціальних символів.
13. Довжина пароля в Систему повинна бути не менше 8 знаків, пароль повинен змінюватись не рідше 1 разу на три місяці.
14. Не використовуйте «прості» паролі типу Qq123456, abcd1234, P@ssword та похідні від них, типу Qq123456!, abcd!234, Passw0rd.
15. Перед початком роботи з Системою і введенням логіну та паролю на сторінці авторизації, переконайтеся, що Ви саме на сторінці банку.
16. Переконатися, що Ви на правильній сторінці, можна перевіривши також сертифікат, за допомогою якого здійснюється захищене з'єднання. Відмітка, що визначає захищене з'єднання, найчастіше виглядає як «замок». У вікні властивостей сертифіката, який відкриється, ви зможете переконатися, кому він був виданий.
17. Ніколи не відкривайте сайт Системи по посиланнях на сторонніх сайтах або отриманим по електронній пошті, СМС і т.п. Для зручності використання введіть адресу сайту Системи самостійно і додайте цю сторінку в закладки браузера.
18. У параметрах браузера необхідно здійснити настройку таким чином, щоб заборонити виконувати:
    - автоматичне завантаження файлів з мережі Інтернет;
    - автоматичний запуск файлів з мережі Інтернет;
    - сценарії і завантаження елементів ActiveX.
19. Не використовуйте функцію «запам'ятовування пароля» в браузерах.
20. По закінченню роботи з Системою, обов'язково здійснюйте безпосередній вихід натиснувши відповідну кнопку «Вийти».

!!! Пам'ятайте, що будь-яка особа, яка має безпосередній доступ до комп'ютера, ноутбука, смартфону, за допомогою якого ви здійснюєте роботу з Системою, може встановити на нього шкідливе програмне забезпечення і заволодіти Вашими даними для доступу до Системи.