



Рекомендації клієнтам щодо безпечного використання систем дистанційного обслуговування банку

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб при роботі з системами дистанційного обслуговування рахунків (далі – СДБО), розроблено ряд рекомендацій:

1. Обмежте доступ сторонніх осіб до пристрою, на якому виконується робота зі СДБО (персонального комп'ютера, ноутбука, смартфона, планшета, тощо). У разі втрати пристрою або у разі будь-якої підозри на компрометацію особистих ключів для роботи зі СДБО необхідно негайно сповіщати про це контакт-центр банку за номером телефону 0 800 210 804 (безкоштовно в межах України) або +38 044 205-33-76 (за тарифами оператора).
2. Налаштовуйте окремо мережеве обладнання корпоративних і персональних комп'ютерів. Доступ до мережі Інтернет обмежуйте «білим списком» сайтів з усіх робочих місць, на яких здійснюється підготовка, підписання та відправлення платіжних документів. Радимо виконувати перевірку кому та ким виданий сертифікат надійності сайту, на якому переглядаєте інформацію, а також стежити за строком його дії. Натиснувши на значок замка можна переглянути властивості сертифікату.
3. Користувачу не рекомендується встановлювати програмне забезпечення (додатки), в тому числі мобільний додаток CARBank, завантажені з невідомих джерел/вебсайтів і не відкривати файли, отримані з ненадійних джерел, надіслані електронною поштою від невідомих відправників. Використовувати ліцензійне програмне забезпечення для захисту від зловмисного коду, регулярно поновлювати антивірусні бази та регулярно здійснювати перевірку свого пристрою на наявність вірусів та шпигунських програм.
4. Тримайте у таємниці та не повідомляйте стороннім особам свій логін, пароль, пароль з СМС-повідомлення, які використовуються для доступу до СДБО.
5. Завжди контролюйте стан рахунків.
6. Після закінчення роботи зі СДБО обов'язково вийдіть з системи, щоб сторонні особи не змогли скористатися нею.

7. Нікому не передавайте управління своїм обліковим записом в СДО.

8. Нікому не передавайте в будь-якій формі свої логін та пароль до облікового запису в СДО.

9. Забезпечте захист свого мобільного телефону та SIM-картки, на номер якої СДО надсилає коди підтвердження операцій.

10. Забезпечте антивірусну безпеку своїх інформаційних систем (на персональних комп'ютерах, смартфонах, планшетах і т.п.), за допомогою яких виконується доступ до СДО.

11. Негайно змініть пароль в СДО, якщо пароль або його частина стала відома іншій особі.

12. Не рекомендується працювати із системою CAPiBank:

- в інтернет-кафе, публічних місцях, використовуючи публічні відкриті Wi-Fi-мережі, де немає гарантії того, що за вашими діями не стежить стороння людина;
- якщо Ви не впевнені в безпеці встановленого програмного забезпечення, а саме у відсутності вірусів, троянів, кейлоггерів – програм, що пересилають паролі користувача третім особам);
- на комп'ютерах, що перебувають у користуванні інших осіб (робочий комп'ютер на кілька користувачів, комп'ютер у бібліотеці, навчальному закладі, державній/приватній установі тощо);
- у місцях, де встановлені пристрої відеоспостереження, за допомогою яких можна отримати інформацію про ваші введені паролі.

В разі виявлення здійснення несанкціонованого доступу до облікового запису в СДО, компрометацію мобільного додатку або його злам, негайно зверніться до Контакт - Центру за телефонами 0 800 210 804 (безкоштовно в межах України) або +38 044 205-33-76 (за тарифами оператора).

Пам'ятайте! АТ «БАНК «УКРАЇНСЬКИЙ КАПІТАЛ» ніколи не здійснює дзвінки та розсилку електронних листів з проханням надати конфіденційну інформацію про логіни, паролі або інші конфіденційні дані.