АСВІО БАНК

РЕКОМЕНДАЦІЇ ТА ПОВІДМЛЕННЯ ЩОДО БЕЗПЕЧНОГО ВИКОРИСТАННЯ СИСТЕМИ ДИСТАНЦІНОГО ОБСЛУГОВУВАННЯ (СДБО) АТ «АСВІО БАНК»

1. Використовуйте лише ліцензійне програмне забезпечення на робочих станціях.
2. Для отримання доступу до СДБО, використовуйте персональний комп'ютер або інший, зокрема мобільний, пристрій, що забезпечує доступ до мережі Інтернет.
3. Використовувати ліцензійне антивірусне програмне забезпечення та своєчасно виконувати оновлення антивірусних баз.
4. Під час роботи з системою СДБО не використовувати комп'ютер для перегляду Інтернет - ресурсів, не пов'язаних з роботою, не відвідувати сайти зі сумнівним змістом, які найчастіше є джерелом поширення шкідливих програм (ураження відбувається непомітно для користувача).
5. Уникайте використання роботи із СДБО в публічних місцях, з чужих ноутбуків та комп'ютерів, смартфонів та інше. Якщо вхід у СДБО здійснюєте в публічних місцях, Клієнт перед закриттям вікна браузера очистіть буфер браузера та видаліть тимчасові файли та cookies.
6. Не відповідайте на підозрілі листи з проханням надіслати пароль та інші конфіденційні дані.
7. Не залишайте персональний комп'ютер (інший пристрій, з якого здійснюється доступ до Системи) без нагляд.
8. Закінчувати поточну сесію (тобто, закінчувати роботу з СДБО) через посилання «Вихід» та закривайте вікно веб- браузера.
9. Регулярно (не рідше, ніж раз на тиждень) здійснюйте повне сканування персонального комп'ютера (іншого пристрою) для виявлення вірусів та зловмисного програмного забезпечення.
10. Міняйте пароль, у випадку отримання таких рекомендацій від Банку.
11. Зберігайте в таємниці дані з автентифікації, а мобільний телефон (SIM-карта, що відповідає Номеру мобільного телефону Клієнта) – під постійним особистим контролем Клієнта. При використанні даних з автентифікації необхідно Логін та Пароль зберігати окремо.
12. При генерації паролів дотримуйтеся політики паролів:

- паролі повинні бути унікальні для кожного Клієнта протягом усього часу роботи системи, містити тільки латинські букви різних регістрів, цифри і допустимі символи: @ # $% * () _ - + = |. Усі інші символи, пробіл та інші мови (не латинські) є недопустимими;
- не рекомендується генерувати пароль для входу в СДБО використовуючи значення або ім'я, пов'язане з користувачем (ім'я, прізвище, ім'я дружини, дітей тощо), послідовность знаків, що повторюються (наприклад, «access»), очевидних послідовностей та узорів, які створюються символами, нанесеними на клавіші клавіатури (наприклад, qwert або zxcvb);
- пароль повинен бути довжиною не менше 8 символів і задовольняти вимогам по його складності тобто одночасно містити як великі, так і маленькі букви, цифри.

13. Негайно повідомляйте Банк, якщо вважаєте, що його персональна інформація була скомпрометована.
14. Видаляйте підозрілі електронні листи без їх відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *.exe, *.pif, *.vbs та інші файли.
15. У разі виявлення будь-якого зловмисного програмного забезпечення (віруси, троянські програми тощо) на робочій станції, здійсніть вхід в СДБО із гарантовано незараженої робочої станції та замінити пароль доступу до СДБО.
16. При виявленні спроби несанкціонованого доступу до СДБО терміново змініть Пароль для входу до СДБО та зверніться до Контакт – центру Банку для блокування доступу до СДБО. Рекомендується також провести сканування робочої станції на виявлення вірусів та іншого зловмисного програмного забезпечення.
17. У випадку виникнення будь-яких підозр щодо компрометації паролей (копіювання, втрату тощо), несанкціонованого доступу до СДБО чи компрометування мобільного телефону, який використовується для отримання паролей – обов'язково змініть пароль чи заблокуйте СДБО та повідомте Банк.
18. У випадку зміни Ваших особистих даних в системі дистанційного обслуговування банку, зверніться до Банку для оновлення даних.
19. Не використовуйте банерні посиланням або посиланнями, отриманими електронною поштою при користуванні СДБО Клієнту.