

## **Рекомендації з безпечного використання СДБО AP Bank Шановний Користувач AP Bank!**

З метою безпечного використання системи дистанційного банківського обслуговування AP Bank (далі – СДБО AP Bank або AP Bank) просимо слідувати наступним рекомендаціям:

1. Нікому та ні за яких обставин не повідомляйте паролі та логіни в будь-який спосіб. Якщо Ви отримали електронний лист (у тому числі з будь-якої адреси Банку) з проханням повідомити або підтвердити Ваш логін або пароль – не відповідайте на запит. Пам'ятайте, Банк ніколи не запитує дані Користувача щодо логіну та паролю. Зателефонуйте до служби технічної підтримки користувачів Банку за номером телефону 0 800 300 170 (безкоштовно по Україні) або +38 (044) 392 93 73 та повідомте про інцидент.
2. Нікому не повідомляйте та зберігайте в режимі секретності Ваші логіни, паролі, коди, які Ви використовуєте у роботі із СДБО AP Bank.
3. У разі втрати мобільного телефону з Вашим фінансовим номером телефону (SIM-карти), негайно заблокуйте SIM-карту (номер телефону) та заблокуйте свій профіль в СДБО AP Bank шляхом звернення до технічної підтримки користувачів Банку за номером телефону 0 800 300 170 (безкоштовно по Україні) або +38 (044) 392 93 73.
4. Не здійснюйте роботу із СДБО AP Bank з комп'ютерів/гаджетів інтернет-кафе, готелів або інших осіб, оскільки Ви не можете бути впевненими, що вони відповідають вимогам безпеки та захисту Ваших даних. Такі комп'ютери/гаджети можуть бути заражені зловмисними програмами.
5. На час запланованої довготривалої перерви у роботі із СДБО AP Bank, будь ласка, зверніться до технічної підтримки Користувачів AP Bank та заблокуйте тимчасово свій профіль.
6. Під час роботи із ВЕБ сервісом AP Bank періодично перевіряйте адресу сторінки AP Bank (<https://online.ap-bank.com/>). У рядку адреси сторінки у браузері має бути присутнє зображення зачиненого замка. У разі виявлення підозрілих сайтів, оформлення яких схожі зі сторінкою AP Bank, негайно зателефонуйте до технічної підтримки користувачів.
7. Не встановлюйте на мобільному пристрої (смартфоні, планшеті, тощо), на якому встановлено AP Bank програмне забезпечення/додатки з неофіційних джерел, на персональному комп'ютері неліцензійні операційні системи та неліцензійне програмне забезпечення.

8. Дотримання режиму захисту інформації та своєчасне виявлення факту компрометації Ваших автентифікаційних даних дозволить мінімізувати ризики використання СДБО.
9. Використовуйте сучасне антивірусне забезпечення, оновлюйте та проводьте антивірусну перевірку на персональних комп'ютерах та мобільних пристроях.
10. Не залишайте без нагляду Ваш мобільний телефон, планшет, ноутбук або комп'ютер під час роботи з AP Bank.
11. Обов'язково використовувати кнопку «Вихід» після закінчення роботи AP Bank.
12. Не слід здійснювати установку та оновлення будь-якого програмного забезпечення не з офіційних сайтів виробників.
13. Відключіть функцію запам'ятовування паролів у браузерях за допомогою яких Ви працюєте з AP Bank.
14. Для входу до AP Bank завжди використовуйте власні логін і пароль.
15. Не відвідуйте сайтів та будь-яких інших інтернет-ресурсів сумнівного змісту з персонального комп'ютера чи мобільного пристрою на якому використовується AP Bank.
16. Не читайте пошту та не відкривайте поштових вкладень до електронних листів, які надійшли від невідомих або підозрілих адресатів.
17. Забезпечуйте своєчасне встановлення оновлень безпеки програмного забезпечення комп'ютерів/мобільних пристроїв. Необхідно встановити надійні паролі доступу на вхід до персонального комп'ютера/мобільного пристрою, забезпечити періодичну зміну цих паролів.
18. Пам'ятайте про Правила користування платіжною картою, емітованою АТ «АГРОПРОСПЕРІС БАНК». За потреби, повторно ознайомтесь з цими правилами та користуйтеся рекомендаціями по проведенню розрахунків з використанням картки.
19. Додаткова інформація «Про безпеку електронних платежів та карткових розрахунків» розміщена на офіційному сайті Банку за посиланням <https://ap-bank.com/cards-for-individual>

