Технічна підтримка користувачів АР Bank
0 800 300 170 (безкоштовно по Україні)
+38 (044) 392 93 73 (за тарифами Вашого оператора)

Інструкція користувача з безпечного використання системи дистанційного банківського обслуговування АР Bank

Шановний користувач АР Bank!

З метою безпечного використання системи дистанційного банківського обслуговування АР Bank (далі – АР 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 (зокрема, 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 АР Bank та повідомте про інцидент.
2. Нікому не повідомляйте та зберігайте в режимі секретності Ваші логіни, паролі, коди, які Ви використовуєте у роботі з АР 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 АР Bank шляхом звернення до технічної підтримки користувачів АР Bank.
4. Не здійснюйте роботу з АР Bank з комп'ютерів або мобільних пристроїв інтернет-кафе, готелів або інших осіб, оскільки Ви не можете бути впевненими, що вони відповідають вимогам безпеки та захисту Ваших даних. Такі пристрої можуть бути заражені зловмисними програмами.
5. На час запланованої довготривалої перерви у роботі з АР Bank, будь ласка, зверніться до технічної підтримки користувачів АР Bank та заблокуйте тимчасово свій профіль.
6. Під час роботи з вебсервісом АР Bank періодично перевіряйте адресу сторінки АР 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 АР Bank, негайно зателефонуйте до технічної підтримки користувачів.
7. Не встановлюйте на мобільному пристрої, на якому встановлено АР Bank, програмне забезпечення 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 АР Bank.
9. Використовуйте сучасне антивірусне забезпечення, оновлюйте та проводьте антивірусну перевірку на персональних комп'ютерах та мобільних пристроях.
10. Не залишайте без нагляду персональний комп'ютер або мобільний пристрій під час роботи з АР Bank.
11. Не здійснюйте установку та оновлення будь-якого програмного забезпечення не з офіційних сайтів виробників.
12. Відключіть функцію запам'ятовування паролів у браузерах, за допомогою яких Ви працюєте з АР Bank.
13. Для входу до АР Bank завжди використовуйте власні логін і пароль.
14. Не відвідуйте сайти сумнівного змісту з персонального комп'ютера або мобільного пристрою, на якому використовується АР Bank.
15. Не читайте електронні листи та не відкривайте вкладення до електронних листів, які надійшли від невідомих або підозрілих адресатів.
16. Забезпечуйте своєчасне встановлення оновлень безпеки програмного забезпечення персональних комп'ютерів або мобільних пристроїв. Встановіть надійні паролі доступу на вхід до персонального комп'ютера або мобільного пристрою, періодично змінюйте ці паролі.
17. Пам'ятайте про правила користування пластиковою платіжною карткою та рекомендації з безпеки електронних платежів та карткових розрахунків. За потреби, повторно ознайомтесь з цими правилами та користуйтесь рекомендаціями по проведенню розрахунків з використанням картки. Дана інформація розміщена на офіційному сайті Банку у розділі Картки для приватних осіб.