Comin Bank
Комерційний Індустріальний Банк

ПАМ'ЯТКА КЛІЄНТА
з питань безпеки використання системи дистанційного банківського обслуговування

Увага!!! Будь ласка, не ігноруйте текст нижче (для обов'язкового прочитання)

При здійсненні операцій засобами дистанційного банківського обслуговування:

1. Зберігайте у режимі суворої секретності Ваші аутентифікаційні дані: логіни, паролі, PIN-коди, TouchID, - які Ви використовуєте у роботі із сервісами системи дистанційного банківського обслуговування (далі - Система). Ніколи не зберігайте їх на SIM-картах, flash-накопичувачах і жорстких дисках Вашого мобільного телефону, планшету, ноутбуку або комп'ютера.

2. Нікому (у тому числі, і працівникам Банку) та ні за яких обставин не повідомляйте паролі та логіни по телефону або у поштовому повідомленні. 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. Зателефонуйте до служби підтримки клієнтів Банку та залиште повідомлення про спробу несанкціонованого отримання Ваших аутентифікаційних даних. Не надсилайте з власної ініціативи без прохання працівника служби підтримки отриманий лист на адреси Банку.

3. Пам'ятайте, що Банк ніколи не запитує та не повідомляє (!) паролі у телефонному режимі або електронною поштою.

4. Відключіть функцію запам'ятовування паролів у браузерах (Internet Explorer, Google Ghrome, FireFox, Opera тощо) на мобільному телефоні, планшеті, ноутбуку і комп'ютері, з допомогою яких Ви працюєте з Системою.

5. Для входу у Систему завжди використовуйте власні логін і пароль.

6. Не залишайте без нагляду Ваш мобільний телефон, планшет, ноутбук або комп'ютер під час роботи з Системою.

7. У разі втрати мобільного телефону, на який Ви отримуєте SMS-повідомлення з одноразовими паролями, негайно заблокуйте SIM-карту (номер телефону).

8. На час довготривалого (декілька місяців і більше) перериву у роботі із Системою, зверніться до служби підтримки клієнтів Банку та заблокуйте свій логін.

9. Не здійснюйте роботу із Системою з комп'ютерів інтернет-кафе, бізнес-центрів, готелів, ігрових залів або інших осіб, оскільки Ви не можете бути впевненими, що вони відповідають вимогам безпеки та захисту Ваших даних. Такі комп'ютери можуть бути заражені програмами для пошуку і крадіжки паролів, номерів платіжних карт тощо.

10. Під час роботи із сервісом Інтернет-банкінгу періодично перевіряйте чинність адреси сторінки Системи (https://cib-online.com.ua). У рядку адреси сторінки у Вашому браузері має бути присутнє зображення зачиненого замка. Рядок адреси сторінки в браузері Internet Explorer має бути підсвічено зеленим кольором. У разі виявлення підозрілих сайтів, імена яких та стиль оформлення схожі зі сторінкою Системи, негайно зателефонуйте до служби підтримки клієнтів Банку та залиште повідомлення про спробу фальсифікації сайту Системи.

11. Не відвідуйте сайтів сумнівного змісту та будь-яких інших Інтернет-ресурсів (соціальні мережі, конференції та чати, телефонні сервіси тощо) з персонального комп'ютера чи мобільного пристрою, на якому здійснюється підготовка та відправка документів до Банку. Не читайте пошту та не відкривайте поштових вкладень до електронних листів, які надійшли від невідомих або підозрілих адресатів. Не слід здійснювати установку та оновлення будь-якого програмного забезпечення не з офіційних сайтів виробників.

12. Використовуйте сучасне антивірусне забезпечення, оновлюйте та проводьте антивірусну перевірку на персональних комп'ютерах та мобільних пристроях. Наголошуємо, що шкідливе

програмне забезпечення здатне перехоплювати будь-які дані з персональних комп’ютерів і мобільних пристроїв, зберігати і поширювати таку інформацію для подальшого несанкціонованого використання сторонніми особами злочинним шляхом.

13. Забезпечуйте своєчасне встановлення оновлень безпеки операційної системи, браузерів та програмного забезпечення комп’ютерів/мобільних пристроїв. Необхідно встановити надійні паролі доступу на вхід до персонального комп’ютера/мобільного пристрою, забезпечити періодичну зміну цих паролів.

14. Пам’ятайте, що дотримання режиму захисту інформації та своєчасне виявлення факту компрометації Ваших аутентифікаційних даних дозволить мінімізувати ризики отримання збитків та усунути чинники загроз.