БЕЗПЕКА РОБОТИ З СДБО

СДБО – Система дистанційного банківського обслуговування, програмне забезпечення також відоме як Клієнт-банк.

Під час підключення до **мереж Wi-Fi в публічних місцях** уникайте використання СДБО !

Виконуйте обов'язковий вихід із СДБО по закінченню роботи з ним натиснувши в інтерфейсі відповідну кнопку - «Вийти»!

Правила роботи з ключами СДБО:

- **Не передавайте ключі стороннім особам!** На власнику ключа - персональна відповідальність за його зберігання та використання!
- **Не копіюйте файли з ключем зі змінного носія** (flash-usb) на ПК/ноутбук тощо.
- **Для надійності зберігання ключів, використовуйте спеціалізовані апаратні носії ключів (USB-токен), що забезпечують захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значеннями параметрів особистих ключів та від їх копіювання.**
- **Не залишайте носій з ключем вставленим у ПК** після завершення роботи з СДБО, щоб уникнути компрометації або втрати/крадіжки ключа!

Багатофакторна автентифікація - це розширена автентифікація, метод контролю доступу до СДБО та підтвердження платежів. **Не нехтуйте нею!**

Усі заходи безпеки спрямовані на підвищення захисту Ваших даних та коштів!

У випадку виявлення фактів несанкціонованого переказу коштів з Ваших рахунків, **просимо терміново в будь який час повідомити** про цей факт працівника відділення на якому Ви обслуговуєтеся, **або зателефонувати до Банку** за номером: **0 800 503 580** або **044 393 25 90**!

ПРАВИЛА РОБОТИ З СДБО

На ПК/ноутбуку де встановлено СДБО :

- **Використовуйте виключно ліцензоване ПЗ** (у тому числі ОС та антивірус) та слідкуйте за його оновленням! Неактуальні версії ПЗ вразливі до зараження комп'ютерними вірусами, програмами-шпигунами, програмами-вимагачами тощо.
- **Не дозволяйте довіреним особам, близьким, рідним працювати з технікою де встановлено СДБО**! Це може призвести до негативних наслідків (викрадення облікових даних або параметрів доступу, зараження ПК тощо).

Надійно зберігайте паролі:

- **Нікому не повідомляйте** паролі доступу до ключа та одноразові паролі банків.
- **Не діліться паролями через електронну пошту** або повідомлення.
- **Не записуйте свої паролі на наліпці** на ПК/ноутбуку.
- **Не зберігайте паролі в нотатках** на смартфоні або ноутбуку.
- **Не зберігайте паролі у браузерах** (якщо при спробі ввести пароль на вебсайті ваш браузер запропонує зберегти його. Якщо погодитись – при реалізації негативного сценарію зловмисники зможуть скористатись цим).

У випадку виявлення фактів несанкціонованого переказу коштів з Ваших рахунків, **просимо терміново в будь який час повідомити** про цей факт працівника відділення на якому Ви обслуговуєтеся, **або зателефонувати до Банку** за номером: **0 800 503 580** або **044 393 25 90**!

ЗАХИСТ ВІД ФІШИНГУ

Фішинг - вид шахрайства або форма кібератаки за допомогою соціальної інженерії, метою якого є обман жертви зловмисником, який видає себе за надійне джерело.

При отриманні листів по e-mail або повідомлень в месенджері:

- **Не переходьте** за підозрілими та неперевіреними посиланнями* в листах та повідомленнях!
- **Не відкривайте** вкладень, що надходять з невідомих адрес!

* - перевірити посилання на предмет фішингу можна на ресурсі «**VirusTotal**» (за адресою https://www.virustotal.com/)

При отримання електронної пошти або використанні Інтернет:

- **Уважно перевіряйте адресу відправника!** Часто зловмисники маскуються під Податкову, СБУ, Банк або інші установи та їх представників, щоб завоювати вашу довіру.
- **Не вводьте жодних даних на ресурсах у яких ви не впевнені** (логіни, паролі, номери рахунків), або на сторінках з посилань які надійшли з невідомих адрес.
- **Не відповідайте на листи з проханням вислати будь-які персональні данні**, логіни та паролі від СДБО, або одноразові паролі. Банк ніколи не здійснює розсилку електронних листів, SMS чи інших повідомлень із вимогою уточнити чи надати Ваші конфіденційні дані.

У випадку виявлення фактів несанкціонованого переказу коштів з Ваших рахунків, **просимо терміново в будь який час повідомити** про цей факт працівника відділення на якому Ви обслуговуєтеся, **або зателефонувати до Банку** за номером: **0 800 503 580** або **044 393 25 90**!