Рекомендації щодо безпечного використання системи дистанційного банківського обслуговування «Клієнт-Банк»

Шановні клієнти!

У зв'язку зі зростанням кількості кіберзлочинів, пов'язаних з несанкціонованим переказом коштів з рахунків клієнтів, які обслуговуються за допомогою систем дистанційного банківського обслуговування, та з метою попередження можливих збитків від шахрайських дій сторонніх осіб, **наполегливо просимо Вас** під час використання системи «Клієнт-Банк» (далі – СКБ) **дотримуватись** нижченаведених організаційних та технологічних **заходів безпеки**.

1. **Доступ до комп'ютеру, на якому встановлено програмне забезпечення СКБ, повинні мати лише ті особи, які вповноважені здійснювати підготовку, підписання та відправлення документів до Банку, згідно відповідних розпорядчих документів Клієнта**, тому:

– **обмежте кількість персональних комп'ютерів**, на яких інстальовано програмне забезпечення СКБ, відповідно до службової необхідності Вашої організації;

– **обмежте кількість користувачів комп'ютерів**, на яких здійснюється підготовка та відправлення документів до Банку, виключно відповідальним працівникам, які безпосередньо уповноважені та мають право проводити роботи з програмним забезпеченням СКБ;

– встановлюйте **надійні паролі доступу**[1] на вхід до персональних комп'ютерів, на яких інстальовано програмне забезпечення СКБ, та обов'язково **забезпечуйте їх періодичну зміну** (не рідше, ніж раз на 6 місяців);

Примітка 1

Для створення надійного паролю доступу варто керуватися наступними принципами:

- *пароль повинен містити не менше 8 символів;*
- *пароль повинен містити літери як верхнього (A-Z), так і нижнього регістру (a-z), числа (0-9), а також спец символи (@, ! тощо);*
- *НЕ слід використовувати в якості пароля своє ім'я або прізвище, дату свого народження тощо;*
- *НЕ використовуйте найпоширеніші паролі: qwerty, 123456, 098765, 1111, password тощо;*
- *НЕ записуйте паролі в блокнотах, на папірцях, у текстових файлах.*

Запам'ятайте свій пароль і ніколи нікому його не передавайте!

– за можливості, **обмежте фізичний доступ** до персональних комп'ютерів, на яких здійснюється підготовка та відправлення платіжних документів до Банку.

2. Згідно умов Договору на розрахункове обслуговування з використанням системи «Клієнт-Банк» (далі – Договір) **Клієнт зобов'язаний самостійно забезпечувати антивірусний захист комп'ютера**, тому:

– забезпечуйте **належний антивірусний захист** комп'ютерів, на яких інстальовано програмне забезпечення СКБ, використовуючи **сучасне антивірусне програмне забезпечення**, для якого **постійно надходять оновлення** антивірусних баз даних, та проводьте **періодичні перевірки** цих комп'ютерів на наявність зловмисного коду (щонайменше 1 раз на місяць);

– забезпечуйте **своєчасне встановлення оновлень безпеки** операційної системи, браузерів та іншого програмного забезпечення комп'ютерів, на яких здійснюється підготовка та відправлення платіжних документів до Банку;

– **не використовуйте** на комп'ютерах, на яких здійснюється підготовка та відправлення платіжних документів до Банку, системне або прикладне **програмне забезпечення, для якого** офіційно **припинено підтримку** виробника (не надходять більше оновлення безпеки, що усувають наявні технічні вразливості);

– **не встановлюйте** жодне **неперевірене або неліцензійне програмне забезпечення**, наприклад, завантажене з ресурсів безкоштовного файлового обміну у мережі Інтернет;

– **здійснюйте установку та оновлення** будь-якого програмного забезпечення лише **з офіційних сайтів виробників**;

– **унеможливлюйте** (або суттєво обмежуйте) **відвідування Інтернету** з персонального комп'ютеру, на якому здійснюється підготовка та відправлення платіжних документів до Банку;

– **не відвідуйте сайтів сумнівного змісту** та/або будь-яких інших Інтернет-ресурсів **невиробничого характеру** (соціальні мережі, конференції та чати, телефонні сервіси т.п.);

– **не читайте** пошту та **не відкривайте** поштових вкладень до **електронних листів, які надійшли від невідомих або підозрілих адресатів**;

– **налаштовуйте окремо** мережеве обладнання корпоративних і персональних комп'ютерів;

– **доступ** до мережі Інтернет з усіх робочих місць, на яких здійснюється підготовка, підписання та відправлення платіжних документів, **обмежуйте «білим списком» сайтів**, до якого повинні включатися **виключно перевірені сайти** самої організації, банків, податкової служби, інших державних органів, сервери оновлень системного та антивірусного програмного забезпечення тощо.

Примітки 2

Наголошуємо, що шкідливе програмне забезпечення здатне перехоплювати будь-які дані з персональних комп'ютерів клієнтів та зберігати/поширювати таку інформацію для подальшого несанкціонованого використання сторонніми особами злочинним шляхом.

3. Згідно умов Договору **Клієнт зобов'язаний самостійно забезпечувати належне зберігання носіїв ключової інформації та забезпечувати неможливість доступу до них третім особам,** тому:

– **не допускайте несанкціонованого використання ключів** електронного підпису та **зберігайте ключові носії** у спосіб, що **виключає несанкціонований доступ** до них;

– **зберігайте носії із секретними ключами виключно у тих осіб**, **що** були **призначені відповідальними за використання цих секретних ключів** відповідно до розпорядчих документів Клієнта;

– **ніколи не зберігайте секретні ключі** підпису першої особи, другої особи та адміністратора **на одному носії,** у будь-яких комбінаціях**;**

– **ніколи не виносьте носії** із секретними ключами **із службових приміщень** Клієнта;

– **зберігайте** особисті секретні ключі **на окремих змінних носіях інформації у опечатаному сейфі**;

– **від'єднуйте** ключові носії від робочого місця та **здійснюйте вихід** із СКБ під час перерв (в незалежності від їх тривалості) або після закінчення роботи із СКБ, з метою недопущення використання СКБ сторонніми особами;

– **ніколи не залишайте носії ключової інформації без особистого нагляду**, в незалежності від часу відсутності;

– **ніколи не записуйте та не зберігайте** разом із носіями ключів **паролі** до особистих секретних ключів;

– **нікому**, зокрема співробітникам Банку[3], **не повідомляйте та не передавайте паролі** до особистих секретних ключів **та носії ключів**;

Примітки 3

*Наголошуємо, що **співробітники Банку** при здійсненні технічної підтримки та наданні консультацій щодо використання СКБ **ніколи не цікавляться інформацією про паролі.***

– виконуйте генерацію секретних ключів **тільки самостійно**.

УВАГА!

У разі виявлення:

- втрати носія секретного ключа та/або пароля до нього;
- компрометації секретного ключа або виникнення підозри про таку компрометацію;
- несанкціонованого доступу до СКБ або виникнення підозри про такий доступ;
- несанкціонованої зміни інформації Клієнта в СКБ або виникнення підозри про таку зміну;
- тощо.

НЕГАЙНО повідомляйте про виявлені факти Службу підтримки Клієнтів для термінового блокування роботи Клієнта в СКБ до з'ясування обставин **за телефонами:**

- (057) 714-00-39;
- (057) 700-96-39;
- 067 573 83 26;
- 050 377 07 69;
- 050 303 50 14.

Примітки 4

Нагадуємо, що відповідно до умов Договору Сторони визнають належним чином оформлений і підписаний електронний документ, створений за допомогою системи «Клієнт-Банк» еквівалентним (відповідним) документу на паперовому носії, належним чином оформленому і підписаному, завіреному підписами уповноважених осіб та мастиковою печаткою, а факт наявності вірних електронних підписів на документі – підставою для виконання пов'язаної з документом фінансової операції.

Тож до моменту повідомлення Банку про факти несанкціонованого доступу до СКБ та/або події, що можуть його спричинити, дії Банку щодо здійснення операцій за рахунками Клієнта на підставі платіжного документа, які надійшли засобами СКБ та пройшли перевірку чинності, є правомірними.

З метою попередження можливих збитків від шахрайських дій сторонніх осіб із використанням системи дистанційного банківського обслуговування просимо Вас неухильно дотримуватись:

– організаційних та технологічних заходів безпеки, передбачених Договором на розрахункове обслуговування з використанням системи «Клієнт-Банк»;

– цих рекомендацій щодо безпечного використання системи «Клієнт-Банк».

Точне виконання цих правил позбавить Вас від проблем і неприємностей та забезпечить безпеку Ваших коштів на поточному рахунку.

Якщо у Вас є якісь сумніви у правильності Ваших дій або неясні питання, ми завжди готові надати Вам допомогу.