Додаток 2
до Правил банківського обслуговування фізичних осіб в
Акціонерному товаристві «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 - 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 (!) конфіденційної інформації, логіни та паролі у телефонному режимі або електронною поштою, не розсилає засобами електронної пошти програмне забезпечення для встановлення на Ваші пристрої.

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. Якщо це можливо, не працюйте на робочому місці з правами адміністратора операційної системи.

11. 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.

12. 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.

13. Не встановлюйте на мобільному пристрої (смартфоні, планшеті тощо, на якому встановлено Систему) програмне забезпечення/додатки з неофіційних джерел, на персональному комп'ютері (з якого здійснюється підключення до Web-інтерфейсу) неліцензійні операційні системи та програмне забезпечення.

14. 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.

15. 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.

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

17. **Рекомендації щодо захисту від фішингу**

Фішинг (англ. phishing, від fishing – рибальство) — це вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів - логінів та паролей. Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій, наприклад, від імені банків. У листі, зазвичай, міститься пряме посилання на сайт, який ззовні не відрізняється від справжнього. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами примусити його зазначити свій логін та пароль, який він використовує для отримання доступу до певного сайту. Отримання конфіденційної інформації користувача дає можливість шахраям використовувати облікові записи та банківські рахунки користувачів в своїх цілях.

17.1. Ознаки фішингових листів:

- Адреса відправника. Фішингові повідомлення, зазвичай, мають вигляд електронного листа, який ззовні не відрізняється від оригінального, відправленого з поштової системи АТ «КІБ». За допомогою шкідливого програмного забезпечення шахраї можуть підмінити електронну адресу, яка відображається в будь-якій поштовій скринці клієнта.
- Екстрений характер повідомлення. З метою збільшення кількості відгуків, зловмисники намагаються надати повідомленням екстрений характер, окреслюючи ліміт часу, і викликати необдумані дії користувача.
- Помилки в темі листа. Як правило, в фішингових листах, в полі «Тема» використовується різний регістр літер, набір літер та цифр, допускаються граматичні або друкарські помилки для уникнення фільтрів поштових програм.
- Гіперпосилання на підроблені сайти. Посилання, зазначені в фішингових листах, ззовні схожі на офіційну веб-адресу АТ «КІБ» і перенаправляють користувачів на веб-сайти, які імітують зовнішній вигляд легітимного сайту Банку.

17.2. Розпізнати підроблений сайт можливо за адресою веб-сайту та за спливаючими вікнами.

Більшість методів фішингу зводиться до маскування підроблених посилань на фішингові сайти під посилання реальних організацій. Шахраї часто використовують адресу з друкарськими помилками або субдомени. В дійсності, адреса сайту (URL) складається з набору цифр та літер і вміст сайту є підробленим. Але частина інформації та некритичні посилання можуть бути оригінальними.

Користуючись різним шкідливим програмним забезпеченням, шахраї мають змогу створювати та розміщувати підроблені спливаючі вікна на основі легітимного сайту, котрі запитують конфіденційну інформацію. При цьому справжній сайт Банку буде відображатись в фоновому режимі. Таким чином, вся, зазначена Вами, інформація в підробленому спливаючому вікні буде доступна шахраям.

17.3. Виконання перерахованих нижче правил дозволить Вам успішно протистояти фішинговим атакам:

- Ніколи не надавайте логін, пароль та інші конфіденційні дані стороннім особам. Не відповідайте на листи з проханням вислати Вашу особисту або фінансову інформацію та не переходьте по вказаних посиланнях, оскільки всі листи, з запитом конфіденційної інформації є шахрайськими.
- Для входу на Web-сторінку Інтернет-банкінгу «CIB-Online» використовуйте лише адресу https://cib-online.com.ua, введену ВРУЧНУ в адресний рядок Вашого браузеру або користуйтесь власними закладками.
- Використовуйте останню версію браузера. Такі браузери як Internet Explorer, FireFox, Google Chrome, Opera систематично оновлюються і мають фільтр захисту від фішингу.
- Завжди перевіряйте, при передачі персональної інформації, та використовуйте шифроване з'єднання. При використанні безпечного з'єднання адреса сайту завжди розпочинається з "https://", а не з http://.

18. Якщо Ви отримали сумнівний електронний лист від імені АТ «КІБ», або виявили фішинговий вебсайт Банку, або виявили несанкціонований доступ та/або зміну ваших даних/інформації в Інтернет-банкінгу «CIB-Online» повідомте про це Контакт-Центр АТ «КІБ» за телефонами 0 800 501 200 (дзвінки безкоштовні у межах України), +38 (044) 290-79-00 (вартість дзвінків згідно з тарифами вашого оператора), або перешліть сумнівний лист/ відповідну інформацію про вебсайт/несанкціонований доступ/зміну вашої інформації з коментарями на електронну адресу: info@cib.com.ua.