BANK ALLIANCE
АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК АЛЬЯНС»

Безпечне використання Клієнтами банківських систем дистанційного обслуговування

Індикатори несанкціонованого втручання в роботу комп'ютера

- Перебій у роботі комп'ютера, раптове перезавантаження системи
- Неможливість або ускладнення запуску програм та додатків
- Наявність невідомих записів в історії входів до системи та проведення операцій
- Раптове уповільнення швидкості роботи комп'ютера, поява незрозумілих вікон
- Самостійний рух по екрану курсора миші з відкриттям вікон, запуском програм тощо
- Сповіщення антивірусного програмного забезпечення про виявлений вірус

Несанкціоноване списання! Що робити?

У разі виявлення несанкціонованого переказу коштів у системі СДО, Клієнту (потерпілому) необхідно:

- Негайно звернутися по телефону або іншим доступним засобом зв'язку до підрозділу Банку, який є відповідальним за обслуговування рахунку
- Повідомити співробітникові Банку *(менеджер, що обслуговує Клієнта, оператор Контакт-Центру, співробітник служби банківської безпеки тощо)* про факт несанкціонованого переказу коштів
- Вимкнути комп'ютер із системою СДО, **примусово знеструмивши його** *(відключити електроживлення в обхід штатної процедури завершення роботи, витягти всі акумуляторні батареї з ноутбука, від'єднати шнур живлення)*
- У випадку роботи з СДО через **віддалений доступ** — терміново завершити сесію. За відсутності можливості знеструмлення комп'ютера — здійснити відключення відповідно до штатної процедури і зафіксувати цей факт
- Негайно сповістити ІТ-підрозділ та внутрішню службу безпеки своєї компанії або директора про інцидент

Хочете уникнути шахрайства в СДО? Правила безпеки (1)

- На робочих місцях використовуйте лише ліцензійне програмне забезпечення
- Користуйтесь ліцензійними антивірусними програмами та своєчасно виконуйте оновлення антивірусних баз
- За жодних обставин не зберігайте таємні ключі на жорсткому диску комп'ютера — лише на зовнішніх носіях *(токени і т. п.)*.
- Після закінчення роботи із системою дистанційного обслуговування та під час перерви від'єднайте носій із секретним ключем від комп'ютера
- Після закінчення роботи із системою дистанційного обслуговування обов'язково здійсніть вихід із системи для недопущення її використання сторонніми особами
- Не використовуйте будь-який віддалений доступ до робочого комп'ютера, на якому встановлено систему дистанційного обслуговування
- У разі будь-якої підозри на компрометацію ключів системи дистанційного банківського обслуговування необхідно негайно сповістіть про це Банк
- Контролюйте стан Вашого поточного рахунку

Хочете уникнути шахрайства в СДО? Правила безпеки (2)

- Не використовуйте комп'ютер із встановленою системою дистанційного обслуговування для перегляду сумнівних та не пов'язаних з роботою інтернет-ресурсів — саме вони найчастіше є джерелом поширення шкідливих програм та непомітного втручання кібер-шахраїв
- Не завантажуйте та не зберігайте на комп'ютері із встановленою системою дистанційного обслуговування підозрілі файли, які отримані з невідомих/підозрілих джерел, надіслані електронною поштою від невідомих адресантів тощо
- Подібні файли слід видаляти або, у разі необхідності завантаження, перевіряти антивірусною програмою
- Зберігайте зовнішні носії ключової інформації *(токени і т. п.)* у сейфі
- Не передавайте стороннім особам носії ключової інформації та не повідомляйте їм паролі доступу до системи дистанційного обслуговування

Хочете уникнути шахрайства в СДО? Правила безпеки (3)

- При виявленні/підозрі про факти доступу сторонніх осіб до ключової інформації негайно ініціюйте блокування та зміну ключової інформації
- Не зберігайте та не записуйте паролі таємних ключів разом із носіями ключів *(токени, usb flash тощо)*
- Уникайте використання для роботи із системою дистанційного обслуговування комп'ютерів, які встановлені у публічних місцях, чужих ноутбуків, смартфонів та планшетів
- **Не відповідайте на підозрілі листи з проханням надіслати секретний ключ електронного цифрового підпису, пароль та інші конфіденційні дані!**

Інструменти безпеки Банку для СДО Клієнта

- SMS-оповіщення клієнта про операції в КБ
- Двохфакторна автентифікація:
  1. *Підтвердження входу до системи КБ кодом із SMS-сповіщення*
  2. *Підтвердження платежів в системі КБ кодом із SMS-сповіщення*
- Встановлення лімітів при SMS-підтвердженні платежів
- Токени для зберігання ключів
- Вхід до КБ iBank2ua з відомих IP-адрес

Правила для запобігання фішингу

- Перевірка точної адреси офіційного сайту Банка https://bankalliance.ua/ для запобігання крадіжки облікових даних підробленим веб-сайтом, зовнішній вигляд якого повністю копіює дизайн офіційного сайту Банку
- При отриманні листів від невідомих адресатів, які містять посилання на невідомі сайти — ні в якому разі не натискати на них, логіни, паролі, карткові та інші дані не вводити