

ПАМ'ЯТКА

щодо дотримання вимог інформаційної безпеки при використанні Системи клієнт-інтернет-банкінг «ОТР Online»

(обов'язкова до виконання особами, які мають право накладання електронного цифрового підпису на платіжні документи від імені Клієнта, а також особами, які відповідають за експлуатацію та адміністрування комп'ютера (-ів) зі встановленим програмним забезпеченням Системи Клієнт-Інтернет-Банкінг «ОТР Online»)

Ефективність та безпека використання Системи Клієнт-Інтернет-Банкінг «ОТР Online» значною мірою залежить від неухильного дотримання вимог інформаційної безпеки в процесі її експлуатації.

Надаючи зазначену послугу, Банком створено зручну технологію, яка забезпечує надійний захист платежів компанії, за умови недопущення несанкціонованого доступу сторонніх осіб до встановленої на робочому місці Системи Клієнт-Інтернет-Банкінг «ОТР Online», секретних ключів і захисних паролів до них.

Причинами несанкціонованого доступу можуть бути як безпосередній фізичний доступ сторонніх осіб до комп'ютера зі встановленою Системою Клієнт-Інтернет-Банкінг «ОТР Online», так і її зараження комп'ютерними вірусами і троянськими програмами. Чинниками, що сприяють компрометації секретних ключів є залишення носіїв з секретними ключами в USB-портах комп'ютера після закінчення роботи або постійне зберігання секретних ключів на його жорсткому диску.

Зі свого боку Банк вживає усіх заходів для попереджувального реагування на ймовірні загрози інформаційної безпеки та **рекомендує** дотримуватись наступних правил безпечної роботи в Системі Клієнт-Інтернет-Банкінг «ОТР Online»:

Основні правила:

- 1. Обмежте доступ сторонніх осіб до комп'ютера, що використовується Вами для роботи з Системою Клієнт-Інтернет-Банкінг «ОТР Online». Забезпечте безпеку приміщення, в якому вона встановлена.**
- 2. Обмежте доступ сторонніх осіб до мобільного телефонного пристрою, який використовується для отримання одноразових авторизаційних ОТР-Кодів. Нікому не повідомляйте значення одноразового коду. Пам'ятайте, що співробітники Банку не мають права спонукати клієнта повідомляти будь-яким способом значення паролів, кодів, реквізити платежів тощо, а також вимагати проведення будь-яких платежів на користь третіх осіб. Примітка! Не рекомендується використовувати для отримання одноразових авторизаційних ОТР-Кодів номери мобільних телефонів без укладання контракту з операторами мобільного зв'язку.**
- 3. Забезпечте надійне зберігання Секретних Ключів на зовнішньому носії (токені тощо). Не зберігайте файли Секретних Ключів на жорсткому диску комп'ютера. Одразу після проведення операцій з використанням Секретних Ключів, відключайте їхні носії від комп'ютера, не залишайте їх постійно підключеними до комп'ютеру.**
- 4. Використовуйте схему підпису платіжних документів двома підписами (двома ключами) з двох окремих комп'ютерів.**
- 5. Періодично контролюйте стан Ваших поточних рахунків (як мінімум 1 раз на день), навіть якщо Ви особисто не здійснюєте платіжні операції в Системі Клієнт-Інтернет-Банкінг «ОТР Online».**
- 6. Використовуйте тільки ліцензійне програмне забезпечення, отримане з довірених джерел.**
- 7. Використовуйте антивірусне програмне забезпечення та виконуйте своєчасне встановлення оновлень антивірусних баз.**
- 8. Забезпечте своєчасне встановлення оновлень безпеки операційної системи (не рекомендується використовувати операційні системи, підтримка яких розробниками не**

здійснюється (наприклад, Microsoft Windows 98, Microsoft Windows 2000, Microsoft Windows XP тощо)).

9. Активуйте режим фільтрації доступу до Системи Клієнт-Інтернет-Банкінг «ОТР Online» за IP-адресою - штатна функція Системи Клієнт-Інтернет-Банкінг «ОТР Online». Для отримання детальної інформації щодо підключення можливості фільтрації доступу за IP-адресою та здійснення відповідних налаштувань Ваш ІТ-адміністратор має звернутися до Служби Підтримки Системи.
10. Не використовуйте комп'ютер з встановленою Системою Клієнт-Інтернет-Банкінг «ОТР Online» для перегляду інтернет-ресурсів, не пов'язаних з роботою, не відвідуйте сайти зі сумнівним змістом, які найчастіше є джерелом поширення шкідливих програм (ураження відбувається непомітно для користувача).
11. Не встановлюйте і не зберігайте підозрілі файли, отримані з ненадійних джерел, завантажені з невідомих Web-сайтів, надіслані електронною поштою і т.п. Такі файли необхідно негайно видаляти. У разі необхідності завантаження файлу, обов'язково перевіряти його антивірусною програмою перед використанням.

Допоміжні правила:

12. Обмежте доступ до мережі Інтернет з робочого місця, на якому використовується Система Клієнт-Інтернет-Банкінг «ОТР Online», лише необхідним колом довірчих ресурсів (банки, контрагенти тощо).
13. Не працюйте з Системою Клієнт-Інтернет-Банкінг «ОТР Online» під обліковим записом з розширеними правами в операційній системі (наприклад, «Адміністратор»).
14. Відключайте обліковий запис гостьового входу (Guest), виключіть використання режиму автоматичного входу користувача в операційну систему при її завантаженні.
15. При роботі з Системою Клієнт-Інтернет-Банкінг «ОТР Online» використовувати паролі, що відповідають таким вимогам:
 - пароль для входу в Систему Клієнт-Інтернет-Банкінг «ОТР Online» та захисні паролі для секретних ключів встановити відмінним від усіх інших паролів, що використовуються Вами;
 - обирайте паролі достатньої довжини (не менше 6 символів), але який Ви можете запам'ятати (паролі категорично не рекомендується записувати);
 - ніколи не обирайте у якості пароля: дату народження, імена чи прізвища Ваші та Ваших близьких родичів, номер Вашої машини та інші загальновідомі назви/слова, які можна логічним шляхом пов'язати із Вами;
 - намагайтеся уникати використання загальновідомих словоформ, краще використовувати словосполучення;
 - використовуйте великі і маленькі літери, а також цифри.
16. На комп'ютерах зі встановленою Системою Клієнт-Інтернет-Банкінг «ОТР Online» відключайте такі параметри завантаження операційної системи: завантаження із знімного носія (дискета, USB, CD-ROM), завантаження по мережі. Вхід в налаштування BIOS повинен бути захищений паролем, який відомий лише адміністратору системи.
17. Не залишайте без контролю комп'ютери зі встановленою Системою Клієнт-Інтернет-Банкінг «ОТР Online». При тимчасовій відсутності необхідно:
 - a. зберегти та закрити усі відкриті на редагування платіжні документи;
 - b. засобами операційної системи блокувати робоче місце;
 - c. обліковий запис користувача повинен бути захищений паролем;

- d. у налаштуваннях операційної системи повинні бути проставлені налаштування введення пароллю при блокуванні операційної системи;
 - e. вихід з програми Системи Клієнт-Інтернет-Банкінг «ОТР Online» необхідно здійснювати шляхом натискання програмної кнопки «Вихід».
18. Зберігайте зовнішні носії ключової інформації (токени) у сейфі або замкнутому ящику столу.
 19. Не передавайте стороннім особам носії ключової інформації та не повідомляйте їм паролі доступу до Системи Клієнт-Інтернет-Банкінг «ОТР Online». При виявленні фактів доступу сторонніх осіб до ключової інформації (у тому числі, при підозрі такого доступу) негайно ініціюйте блокування та зміну ключової інформації.
 20. Не записуйте і не зберігайте паролі до Секретних Ключів разом з носіями ключів (usb flash, токен і т.п.).
 21. Перевіряйте та не допускайте використання на комп'ютері, на якому встановлено Систему Клієнт-Інтернет-Банкінг «ОТР Online», програмних засобів віддаленого адміністрування (TeamViewer, Remote Desktop Services з клієнтом Remote Desktop Connection, PuTTY, VNC, UltraVNC, Hamachi, Remote Office Manager та ін.). У випадку виявлення такого програмного забезпечення негайно повідомте Банк для блокування Вашого облікового запису в Системі Клієнт-Інтернет-Банкінг «ОТР Online», видаліть виявлене програмне забезпечення та обов'язково перевипустіть Секретні Ключі \ змініть паролі;
 22. Уникайте використання для роботи з Системою Клієнт-Інтернет-Банкінг «ОТР Online» комп'ютерів, встановлених у публічних місцях, чужих комп'ютерів та ноутбуків, смартфонів тощо.
 23. Для комунікації з особами, які мають право підпису платіжних документів, завжди зазначайте у заявці персональні електронні адреси (не використовуйте групові поштові скриньки).
 24. Використовуйте систему захисту від вторгнення в комп'ютерну мережу (Intrusion Prevention System).
 25. Використовуйте мережеві екрани (firewall).
 26. При роботі з електронною поштою і сервісами обміну миттєвими повідомленнями (ICQ, Skype, Mail.Ru-Агент, тощо) звертайте особливу увагу на відправника повідомлення. Якщо відправник Вам невідомий - відкривати вкладення та інші надіслані файли категорично не рекомендується.
 27. Налаштуйте Інтернет-браузер на заборону автоматичного завантаження та запуску файлів з мережі Інтернет;
 28. Якщо у Вас виникла підозра, що Ваш комп'ютер заражений вірусами або іншими шкідливими програмами (неадекватна реакція на Ваші дії, «зависання», незрозуміле уповільнення дії, самостійна активність, поява незрозумілих вікон і т.п.) - негайно повідомте Банк для блокування Вашого облікового запису в Системі Клієнт-Інтернет-Банкінг «ОТР Online», зверніться до системного адміністратора для видалення комп'ютерного вірусу, з подальшим обов'язковим перевипуском Секретних Ключів\зміною паролів;
 29. Не вводьте конфіденційних даних (паролів, ідентифікаторів) у вікна програм, якщо вони відрізняються від стандартних (інші форма, колір, логотипи, написи, шрифти), відображаються не як завжди (в іншому порядку). Уважно читайте усі повідомлення, що виникають на екрані комп'ютеру.

Просимо Вас звернути особливу увагу!

Банк не здійснює розсилку оновлень програмного забезпечення системи Системи Клієнт-Інтернет-Банкінг «ОТР Online» електронною поштою.

Не відповідайте на підозрілі листи з проханням надіслати Секретний ключ електронного цифрового підпису, пароль та інші конфіденційні дані.

У випадку отримання подібних листів просимо Вас звертатися до підрозділів Банку:

- Управління Інформаційної Безпеки на електронну пошту IT.Security@otpbank.com.ua
- Служба підтримки Системи Клієнт-Інтернет-Банкінг «ОТР Online», контактні телефони:
+ 38 044 4900533 та +38 044 4901181, або на електронну пошту clb@otpbank.com.ua.

Сподіваємось, що надана інформація буде корисною для Вас.