ІНФОРМАЦІЯ ПРО БЕЗПЕКУ

Сучасна багатофункціональна система дистанційного обслуговування клієнтів-фізичних осіб дозволяє управляти банківськими рахунками з будь-якої точки світу, використовуючи інтернет. Інтернет-банкінг АТ «МОТОР-БАНК» надає клієнту високий рівень зручності та безпеки. Зокрема, дана система інтернет-банкінгу дозволяє клієнтам дистанційно здійснювати операції з рахунками і картами, переказ коштів по Україні, відкривати і поповнювати депозити, погашати кредити.

Дані Клієнта захищаються спеціальним паролем для входу, який знаєте тільки Ви, а операції виконуються тільки після Вашого підтвердження спеціальним кодом, який направляється на номер мобільного телефону клієнта.

1. Для отримання доступу до Системи Клієнт зобов'язаний використовувати комп'ютер або інший пристрій, що забезпечує доступ до мережі Інтернет, на якому встановлені:
• операційна система (наприклад, Microsoft Windows) з останніми оновленнями;
• остання доступна версія веб-браузера (наприклад, Internet Explorer, Firefox, Chrome, Safari)
• ліцензійне антивірусне програмне забезпечення (наприклад, ESET NOD32, Trend Micro, Norton і т. п.) з останніми оновленнями баз вірусних сигнатур;
• анти-шпигунське програмне забезпечення (antispyware) і програмний персональний мережевий екран (firewall) (наприклад, Norton Internet Security, McAfee Internet Security і т. п.) з останніми оновленнями.

2. Рекомендується регулярно (не рідше, ніж раз на тиждень) здійснювати повне сканування комп'ютера або пристрою для виявлення вірусів і шкідливих програм.

3. Не рекомендується встановлювати на комп'ютер або пристрій програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях і т. д.).

4. Дані аутентифікації повинні зберігатися в таємниці, а мобільний телефон (SIM-карта, відповідна Номеру мобільного телефону Клієнта - під постійним особистим контролем Клієнта. При використанні даних аутентифікації необхідно логін і пароль зберігати окремо.

5. Паролі повинні бути унікальні для кожного Клієнта даного робочого місця протягом всього часу роботи системи, містити тільки латинські букви різних регістрів, цифри і допустимі символи! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Ђ Ѓ , ѓ „ … † ‡ € ‰ Љ ‹ Њ Ќ Ћ Џ ђ ‘ ’ “ ” • – — ™ љ › њ ќ ћ џ Ў ў J ¤ ¦ © ¬ ® ° ± µ № j S s |. Всі інші символи, пробіл та символи (не латинська) інших мов є неприпустимими. Пароль для входу в Систему не повинен містити словникове слово або ім'я, пов'язане з користувачем (ім'я, прізвище, ім'я дружини, дітей і т. п.), не містити повторювані послідовності знаків (наприклад, «access»), очевидних послідовностей і візерунків, які створюються символами, нанесеними на клавіші клавіатури (наприклад, qwert або zxcvb). Пароль повинен бути довжиною не менше 6 символів і задовольняти вимогам його складності, тобто одночасно містити як великі, так і маленькі букви, цифри і спеціальні символи. При зміні пароля він не повинен повторювати 3 останніх пароля.

6. При використанні Системи Клієнт повинен:
• здійснювати підключення до Системи тільки за допомогою перевірених комп'ютерів і пристроїв, уникати підключення з публічних місць (інтернет-кафе, готелі, бібліотеки і т. п.);
• переконатися при вході в Систему, що в адресному полі веб-браузера знаходиться адреса саме Системи "МОТОР Online", а саме https://online.motor-bank.ua/ifobsClientMotor;
• перевіряти надійність постачальника сертифіката ключа, його дійсність і термін дії підтвердженням того, що між веб-браузером Клієнта і веб-сервером Банку встановлено безпечне з'єднання;
• не залишати комп'ютер або інший пристрій, з якого здійснюється доступ до Системи без нагляду;
• завершувати поточну сесію (тобто, закінчувати роботу з Системою) по посиланню «Вихід» і закривати вікно веб-браузера при закінченні роботи в Системі;
• якщо вхід в Систему здійснюється в публічних місцях, рекомендується наявними засобами перед закриттям вікна браузера очистити буфер браузера та видалити тимчасові файли і файли-cookies;
• Не переглядати інші сайти в тому ж браузері, коли Клієнт працює в Системі;
• стежити за тривалістю веб-сесії (тривалістю перебування в Системі без будь-яких дій з боку Клієнта), яка в цілях безпеки обмежена 10 хвилинами;

• для навігації в Системі використовувати виключно посилання і кнопки Системи і не використовувати кнопки навігації браузера (наприклад, Вперед / Назад);
• звертати увагу на повідомлення браузера про небезпеку або помилки.

7. При використанні Системи Клієнту забороняється:
• переходити на стартову сторінку Системи по банерної посиланням або посиланнями, отриманим по електронній пошті;
• відповідати на запити (найчастіше розсилаються по електронній пошті), що містять вимогу надати або перевірити логін, пароль для входу і / або інші дані аутентифікації.

8. Банк ні при яких обставинах не здійснює:
• розсилку електронних листів з вимогою надіслати пароль для входу, логін і / або інші дані аутентифікації і / або не пропонує перейти за вказаною адресою.
• поширення по електронній пошті комп'ютерних програм або персональних відомостей.

9. Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення * .exe, * .bat, * .js, * .vbs, * .apk і інші файли.

10. У разі виявлення будь-яких шкідливих програм (віруси, троянські програми і т. п.) на робочій станції необхідно здійснити вхід в Систему з гарантовано незараженої комп'ютера або пристрою і замінити пароль доступу до Системи.

11. При виявленні спроби несанкціонованого доступу до Системи необхідно терміново змінити пароль для входу в Систему. Рекомендується також провести сканування комп'ютера або пристрою з метою виявлення вірусів та іншого шкідливого програмного забезпечення.

12. Необхідно завжди пам'ятати, що при роботі в Системі завжди залишається ризик компрометації даних аутентифікації і від правильних дій Клієнта залежить можливість звести даний ризик до мінімуму.