KredoBank
PKO Bank Polski Group

РЕКОМЕНДАЦІЇ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

З метою організації безпечної роботи з системою клієнт-інтернет-банк iFOBS необхідно дотримуватись наступних рекомендацій:

1. Ніколи і нікому не розголошуйте свої конфіденційні дані (логін, пароль тощо), навіть особам, що представились співробітниками Банку.
2. Щоб увійти на WEB-сторінку системи клієнт-інтернет-банк ПАТ "Кредобанк" використовуйте лише адресу: **https://ifobs.kredobank.com.ua/ifobsClient/**
3. Не зберігайте таємні ключі, в тому числі паролі до них, на жорсткому диску комп'ютера, де встановлена система клієнт-інтернет-банк iFOBS, тому що це значно збільшує ризик несанкціонованого доступу до ключів сторонніх осіб. Таємний ключ повинен зберігатись виключно на переносних носіях інформації (floppy-дискета, USB-flash накопичувач, CD-диск, тощо).
4. Уникайте використання системи клієнт-інтернет-банк з комп'ютерів в публічних місцях (Інтернет-кафе, бібліотеки), а також на інших комп'ютерах, налаштування яких знаходиться поза Вашим контролем.
5. Обмежте доступ до комп'ютера, який використовується для роботи з системою клієнт-інтернет-банк iFOBS. Обмежте доступ до даного комп'ютера персоналу, який не має відношення до роботи з системою клієнт-інтернет-банк.
6. Доступ до таємних ключів повинен бути тільки в період роботи з системою клієнт-інтернет-банк. Не забувайте виймати зовнішній носій інформації по завершенні роботи з системою iFOBS.
7. Старайтеся регулярно змінювати пароль. Не рекомендується використовувати простих паролів до вашого ключа (своє ім'я чи прізвище, дату народження, одинакові знаки не повинні повторюватися підряд, не мають бути послідовно розміщені на клавіатурі тощо).
8. Використовуйте на робочому місці системи клієнт-інтернет-банк засоби антивірусного захисту та регулярно оновлюйте їх, а також міжмережеві екрани (фаєрволи), анти-шпигунське програмне забезпечення тощо.
9. При виявленні незвичної поведінки системи клієнт-інтернет-банк чи будь-яких змін в інтерфейсі програми – зателефонуйте до Банку та з'ясуйте, чи не пов'язані такі зміни з оновленням програмного забезпечення.
10. При виникненні підозри про здійснення несанкціонованих операцій в системі клієнт-інтернет-банк iFOBS, підозри про несанкціонований віддалений доступ та управління комп'ютером, підозри про компрометацію Ваших конфіденційних даних для входу в систему клієнт-інтернет-банк, негайно повідомте про це ПАТ «КРЕДОБАНК».

Зверніть увагу!

Банк ніколи, за жодних обставин не здійснює розсилку електронних листів, SMS чи інших повідомлень із вимогою уточнити чи надати Ваші конфіденційні дані, оскільки подібні повідомлення є шахрайськими (фішинг).

У випадку виявлення фактів несанкціонованого переказу коштів з Ваших рахунків, просимо терміново повідомити про цей факт працівника відділення, або зателефонувати на інфолінію банку за номером: **0 800 500 8 500** (дзвінки з стаціонарних телефонів безкоштовні).

Скориставшись послугою **Фіксована IP-адреса**, можна обмежити комп'ютери, з яких буде дозволений доступ до системи клієнт-інтернет-банк iFOBS, для здійснення операцій по Вашому рахунку.