ЗАХОДИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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 (системи дистанційного обслуговування «Клієнт-Інтернет-Банк («iFOBS»)) використовуйте лише адресу: https://ifobs.kredobank.com.ua
3. Не зберігайте Особисті робочі ключі, в тому числі паролі до них, на жорсткому диску комп'ютера, з якого відбувається доступ до Системи, тому що це значно збільшує ризик несанкціонованого доступу до Особистого робочого ключа сторонніх осіб. Особистий робочий ключ повинен зберігатись виключно на переносних носіях інформації (floppy-дискета, USB-flash накопичувач, CD-диск, тощо). Зберігайте Особисті робочі ключі в недоступному для сторонніх осіб місці.
4. Уникайте використання Системи 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. Обмежте доступ до даного комп'ютера персоналу, який не має відношення до роботи з Системою.
6. Доступ до ЕЦП на комп'ютері, з якого відбувається доступ до Системи, повинен бути тільки в період роботи з Системою. Не забувайте виймати зовнішній носій інформації з таємними ключами по завершенні роботи з Системою.
7. Пароль до Особистого робочого ключа потрібно регулярно змінювати і він повинен складатися не менше ніж з 8 знаків (цифри, літери), а також не рекомендується використовувати прості паролі (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, з якого відбувається доступ до Системи, засоби антивірусного захисту та регулярно оновлюйте їх, а також міжмережеві екрани (фаєрволи), антишпигунське програмне забезпечення тощо.
9. При виявленні незвичної роботи Системи чи будь-яких змін в інтерфейсі програми – зателефонуйте до Контакт-центру Банку за номером телефону 0800500703 (дзвінки з стаціонарних телефонів безкоштовні) чи за іншим номером, зазначеним на інтернет-сайті Банку (www.kredobank.com.ua) та з'ясуйте, чи не пов'язані такі зміни з оновленням програмного забезпечення.
10. При виникненні підозри про здійснення несанкціонованих операцій в Системі, підозри про несанкціонований віддалений доступ та управління комп'ютером, підозри про компрометацію Особистого робочого ключа, Логіна, пароля негайно зателефонуйте до Контакт-центру Банку (дзвінки з стаціонарних телефонів безкоштовні).
11. Використовуйте послугу SMS-інформування (iFOBS.SMS) про рух коштів на рахунку як оперативний засіб контролю за рухом коштів по рахунку.
12. Забезпечуйте збереження одноразового коду та/або OTP токена таким чином, щоб виключити його використання не уповноваженими особами.

Зверніть увагу!

Банк ніколи, за жодних обставин не здійснює розсилку електронних листів, SMS чи інших повідомлень із вимогою уточнити чи надати Ваші конфіденційні дані (в тому числі Особистого робочого ключа, Логіна, пароля, Одноразового пароля), подібні повідомлення є шахрайськими (фішинг).

БАНК:

_____
(П.І.Б. уповноваженої особи Банку, підпис)

М.П.

КЛІЄНТ:

_____
(П.І.Б. керівника, підпис)

_____
(П.І.Б. гол. бухгалтера, підпис)

М.П.