РЕКОМЕНДАЦІЇ 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 вебсторінку Online Banking використовуйте лише адресу: https://online.kredobank.com.ua/auth/login
3. Ніколи не здійснюйте введення конфіденційної інформації у разі, якщо вас було переадресовано на невідомий вебсайт з незрозумілим доменним іменем.
4. Для завантаження додатків використовуйте виключно Google Play для ОС Android та App Store для ОС iOS.
5. Обмежте доступ до пристроїв, які використовуються для роботи з Системою. Використовуйте на телефоні функцію блокування екрану (Pin Code, Face Id, Touch Id)
6. Уникайте використання Системи в публічних місцях (Інтернет кафе, готелі, транспорт), а також на інших пристроях, налаштування яких знаходиться поза вашим контролем.
7. Пароль повинен складатися не менше, ніж 8 символів. Повинен містити хоча б одну велику та одну маленьку літери, одну цифру і спеціальний символ: ! @ « # № $ % : ; ^ &? * () — _ + =. Пароль не повинен містити будь-які 4 та більше символів з логіну, які розміщені підряд. Наприклад, для логіна Andrii1 пароль не повинен містити Andr, drii, rii1, ndri, і т.д. При зміні паролю не можна використовувати попередній пароль в якості нового.
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 **0 800 500 850** (дзвінки з стаціонарних телефонів безкоштовні) чи за іншим номером, зазначеним на інтернет-сайті банку https://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 чи телефоном, підозри про компрометацію логіна чи пароля, втрати телефона негайно зателефонуйте до Контакт центру банку (дзвінки зі стаціонарних телефонів безкоштовні).

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 логіну, паролю), подібні повідомлення є шахрайськими (фішинг).

З метою унеможливлення потрапляння на фішингові веб-сайти Національний Банк України на своєму офіційному Інтернет-представництві розмістив офіційний

перевірений перелік веб-сайтів банків України. Перевірити автентичність доменного імені та належність веб-сайту конкретній банківській установі можна на сайті НБУ.