Інструкція як подбати про безпеку своїх грошей

Користуючись онлайн-банкінгом або мобільним додатком, завжди дотримуйтесь основних правил безпеки.

- НІКОЛИ та нікому не надавайте свої персональні дані, ідентифікатори чи паролі через Інтернет або по телефону.
- Не встановлюйте програмне забезпечення та не завантажуйте програми з невідомих джерел.
- Не відкривайте електронну пошту від незнайомих відправників, не відкривайте додатки до електронних повідомлень чи СМС-повідомлень, які, на вашу думку, є підозрілими (наприклад, вони надійшли від кур'єрської компанії, хоча ви нічого не замовляли в інтернет-магазинах чи від енергопостачальника, з яким ви не підписували договір).
- Не натискайте на посилання, що ведуть на веб-сторінки ніби-то для оновлення ваших сертифікатів безпеки або системи переказів - банк НІКОЛИ не надсилає таких повідомлень за допомогою електронної пошти.
- Остерігайтеся повідомлень, у яких хтось просить вас доплатити до якоїсь транзакції – переконайтеся, що запит справжній, бажано зателефонувавши особі або компанії.
- Не надсилайте код-BLIK навіть знайомим, які просять вас це зробити через Facebook, месенджер чи іншу соціальну мережу, краще зателефонувати і запитати, чи дійсно вони про це просили.
- Завжди використовуйте актуальні версії операційної системи та застосунків. Захистіть свій комп'ютер за допомогою сучасного антивірусного програмного забезпечення.
- Використовуйте правильні паролі для комп'ютера та онлайн-банкінгу, тобто паролі, які важко розшифрувати. Надійний пароль повинен складатись щонайменше з 8 символів, містити великі та малі літери, цифри та спеціальні символи. Не записуйте свої паролі та не передавайте іншими особам.
- Встановіть безпечні ліміти для інтернет-переказів і карткових платежів. Ви можете легко змінити їх
- в електронному банкінгу.
- Використовуйте електронний банкінг на власному обладнанні та в місці з надійним Інтернетом. Уникайте входу в систему в таких місцях, як кінотеатр, кав'ярня або публічні точки доступу до Інтернету.
- Після завершення використання онлайн-банкінгу, завжди натискайте кнопку «Вийти».
- Під час входу на веб-сторінку інтернет-банкінгу перевірте правильність адреси та шифрування (адреса повинна починатися з https://... , а поруч з нею має бути символ закритого замка). Крім того, перевірте правильність URL-адреси на наявність описок
- і нестандартних символів, які дуже часто не видно на перший погляд.
- Завжди звертайте увагу на повідомлення про недійсність сертифікатів, що відображаються веб-браузером. У випадку сумніві, відмініть транзакцію.
- Не встановлюйте на комп'ютер програми з невідомих джерел.

- Для введення паролю користуйтеся екранною клавіатурою на комп’ютері.
- Слідкуйте за інформацією та повідомленнями, опублікованими на веб-сторінці Банку та надісланими на Вашу скриньку в системі електронного банкінгу.

Якщо Вам зателефонує особа, яка представиться банківським працівником, Ви отримуєте повідомлення, відправники яких видають себе за банк, або якщо щось, пов'язане з переказами, викликає у Вас сумніви, зателефонуйте на нашу гарячу лінію.

ПАМ’ЯТАЙТЕ у разі тимчасової недоступності вашого електронного банкінгу, зберігайте спокій і не панікуйте. Саме це ставлять собі за ціль кіберзлочинці – викликають паніку, страх і хаос. Не допомагайте їм в цьому. Крім того, не керуйтеся анонімними оцінками чи коментарями, наприклад, із соціальних мереж або онлайн-форумів. Переконайтеся, що це достовірна інформація, а не «фейкові новини».