

## **Рекомендації щодо уникнення випадків підвищеного ризику збитків для користувача електронного платіжного засобу (банківської платіжної картки)**

1. Активуйте послугу Надсилання SMS-повідомлень за операціями за картковим рахунком, щоб отримувати SMS-повідомлення про операції за картою, а також для автоматичної та безкоштовної активації послуги 3D Secure (додаткової ідентифікації при здійсненні інтернет-платежів).
2. Захистіть свій фінансовий номер дотримуючись таких рекомендацій:
  - встановіть складний 8-значний номер ПІН-код на SIM-картку;
  - персоналізуйте SIM-картку в оператора мобільного зв'язку;
  - використовуйте окремих номер для банківських операцій, не публікуйте його у соцмережах та не публікуйте і не розповсюджуйте номер картки разом з фінансовим номером телефону. У разі втрати телефону (SIM-картки) або у випадках підозри щодо заволодіння зловмисниками вашим номером телефону, наприклад якщо ваш номер припинив відповідати – негайно повідомте Банк та блокуйте свої картки, зверніться до мобільного оператора про блокування номеру та перевипуск SIM-картки.
3. Тримайте в таємниці свій ПІН-код, в жодному разі не повідомляйте його іншим особам. Конверт або СМС-повідомлення з ПІН-кодом рекомендовано знищити/видалити. В жодному разі не тримайте записаний ПІН-код поряд з картою.
4. Рекомендовано змінювати ПІН-код в банкоматах не рідше ніж раз на три місяці.
5. При отриманні картки поставте власний підпис на зворотному боці картки на панелі для підпису, це зменшить вірогідність використання картки без вашої згоди або в разі її втрати.
6. Тримайте в секреті CVV2-код (три цифри на звороті картки) і в жодному разі нікому не повідомляйте. Рекомендовано його запам'ятати чи записати та після цього стерти зі звороту картки не пошкоджуючи при цьому магнітної стрічки.
7. Здійснюйте операції з використанням карток через банкомати/термінали самообслуговування, які встановлені в безпечних місцях (наприклад, в установах, банках, великих торговельних комплексах, готелях, аеропортах тощо). Не користуйтеся підозрілими банкоматами/терміналами (на яких є предмети, залишки клею або інші сторонні пристрої, що викликають підозру). Не користуйтеся банкоматами/терміналами якщо їх меню підозріле чи незрозуміле.
8. Всі розрахунки картою повинні здійснюватися у вашій присутності, ні за яких обставин не передавайте картку іншим особам. Перед введенням ПІН-коду перевірте правильність введеної на терміналі суми.
9. Збережіть чек за операцією для звірки з випискою в кінці місяця.
10. Контролюйте рух коштів за рахунком шляхом отримання в Банку щомісячної виписки та звіряйте операції.
11. При поповненні картки з використанням її реквізитів (за номером картки) власними коштами пам'ятайте про строки зарахування коштів на картковий рахунок, визначені умовами договору, для уникнення незапланованих розрахунків кредитними коштами або виникнення несанкціонованого овердрафту / понадлімітної заборгованості.

12. Не збільшуйте без потреби ліміти добової активності по картці, робіть це тільки для проведення конкретних операцій.

13. Перед тим як здійснювати розрахунки з використанням реквізитів картки (номер, строк дії, CVV2-код) в мережі Інтернет впевніться в безпеці сайту з дотриманням рекомендацій щодо виявлення фішингових веб-сайтів

14. Запам'ятайте слово – пароль, яке зазначали у Банку при оформленні картки. Слово - пароль обов'язкове для вашої ідентифікації при зверненні до Контактного Центру.

15. Занесіть до телефонної книги, запам'ятайте або занотуйте номери телефонів Контактного Центру 0 800 50 30 05, +380 (44) 207 70 32, щоб у разі необхідності максимально швидко звернутись для блокування картки у разі її втрати тощо.