Перше отримання платіжної картки, платіжних карток:

Одразу після отримання платіжної картки відкрийте конверт з PIN-кодом, запам'ятайте його та знищіть вміст конверта або, у крайньому випадку, збережіть у місці, доступному тільки Вам (сейф).

Не пишіть PIN-код на платіжній картці та не зберігайте записаний PIN-код разом з платіжною карткою на папері або іншому носії інформації.

Запишіть номер своєї платіжної картки та номер телефону філії Банку, де Ви отримали платіжну картку. У випадку втрати платіжної картки Вам слід негайно повідомити Банк за цим номером **+38 (044) 279-51-61.**

Загальні правила користування платіжною карткою:

- Не передавайте платіжну картку в користування іншій особі.
- Нікому не повідомляйте свій PIN-код, навіть дружині, чоловіку, дітям, онукам, співмешканцям, колегам, сусідам, підприємцям.
- Нікому не повідомляйте номер платіжної картки (16 цифр) телефоном, СМС, у листі, окрім випадків, коли Ви особисто зателефонували до Контакт-центру Банку, який видав Вам платіжну картку, та назвали оператору Контакт-центру номер платіжної картки.
- Нікому не повідомляйте CVV2 / CVC2 (код доступу до Інтернет-операції платіжною карткою) телефоном, СМС, у листі.
- Нікому не повідомляйте місяць та рік закінчення строку дії платіжної картки телефоном, СМС, у листі.
- Співробітники Банку або платіжні системи Visa та MasterCard ніколи не запитуватимуть у Вас телефоном, у СМС або в листі номер платіжної картки, CVV2 / CVC2, місяць та рік закінчення строку дії платіжної картки.
- **Якщо співробітники Банку телефонують на Ваш контактний номер телефону, вони запитують лише Ваші прізвище, ім'я, по батькові та дату народження. Ніяких інших даних співробітники Банку не називають і не запитують!**
- Співробітники Банку або платіжні системи Visa та MasterCard ніколи не надсилатимуть Вам у СМС або в листі посилання на сайти, де потрібно ввести дані платіжної картки (номер платіжної картки, CVV2 / CVC2, місяць та рік закінчення строку дії платіжної картки), пам'ятайте, що ці сайти - фальшиві. Згодом отримана інформація використовується для проведення шахрайських операцій Вашою платіжною карткою в Інтернеті.
- Не зберігайте номер платіжної картки, CVV2 / CVC2, місяць та рік закінчення строку дії платіжної картки на папері, в телефоні, смартфоні, планшеті, ноутбуці, домашньому або робочому комп'ютері.
- Не залишайте платіжну картку без нагляду (особливо в торговельних точках, барах, ресторанах, готелях, касах будь-яких установ).
- Перевіряйте рух коштів на Вашому поточному рахунку не менше одного разу на місяць.
- Укладіть з Банком договір для отримання SMS-повідомлень про рух коштів на поточному рахунку: на Ваш мобільний телефон при кожній операції з поточним рахунком надходитиме звіт.
- Змініть кодове слово у відділенні Банку у випадку, якщо Ви отримали платіжну картку на підприємстві.
- Змінюйте кодове слово 1 раз на рік з метою запобігання можливому шахрайству, коли телефонну ідентифікацію проходять підставні особи, які заволоділи Вашими ідентифікаційними даними (кодове слово, номер паспорту, ІПН, дата народження, адреса проживання або прописки).

Заходи безпеки при обслуговуванні в торговельно-сервісних організаціях та відділеннях Банку:

- Не випускайте картку з поля зору (навіть, коли обслуговуючі пристрої знаходяться в іншому приміщенні, візьміть картку та ідіть до іншого приміщення і власноруч проведіть операцію в терміналі).
- Не підписуйте більше двох чеків за однією операцією (при оформленні операції за допомогою механічного пристрою - імпринтеру - не більше трьох). Підпис на чеку - це Ваш дозвіл списати з Вашого карткового рахунку кошти.
- Не підписуйте чек, на якому не вказана підсумкова сума. Підписуючи такий чек, Ви даєте можливість списати з Вашого рахунку будь-яку суму.
- При неправильному оформленні чека вимагайте його анулювання у Вашій присутності. В іншому випадку з Вашого рахунку можуть списати іншу суму.

Заходи безпеки при користуванні банкоматом:

Намагайтеся користуватися одними й тими ж банкоматами, запам’ятати вигляд їх клавіатури та отвору для платіжної картки. Не користуйтесь банкоматом, який Ви не знаєте, оскільки він може містити шахрайські пристрої. Не користуйтесь банкоматом з поганим освітленням, або якщо він знаходиться в глухому, важко доступному місці. Не користуйтесь банкоматом, якщо помітили, що на ньому встановлені зайві пристрої, яких Ви не помічали раніше. Це можуть бути пристрої, встановлені шахраями для отримання даних Вашої платіжної картки або отримання Ваших коштів.

- Якщо Ви помітили, що людина перед Вами використовує багато платіжних карток, а особливо, якщо вони білого кольору, повідомте про це Банк, за затримання такої особи Банк сплатить винагороду. При виявленні невідомого пристрою на банкоматі Банку необхідно повідомити за номером **+38 (044) 279-51-61**, за що Банк сплатить винагороду.
- Не дозволяйте стороннім особам побачити Ваш PIN-код під час його введення, при вводі PIN-коду намагайтесь вільною рукою прикрити клавіатуру так, щоб стороння людина не побачила Ваш PIN-код.
- Намагайтесь не помилятися при вводі PIN-коду, тому що після трьох неправильних спроб платіжна картка може бути заблокована банкоматом.
- Будьте оперативними при роботі з банкоматом та вирішіть наперед, яка сума грошей Вам потрібна.
- На прийняття Вами рішення в кожному пункті меню відводиться близько 30 секунд. Якщо впродовж цього часу Ви не зробите свій вибір, банкомат поверне Вам платіжну картку, а в разі, якщо Ви не заберете платіжну картку, банкомат вилучить її з метою безпеки.
- Після завершення операції перевірте, чи забрали Ви з банкомату платіжну картку, гроші, квитанцію (видається банкоматом на Вашу вимогу).
- Не довіряйте стороннім особам, якщо ті втручаються у Вашу роботу з банкоматом, навіть якщо ці особи (особа) представляються працівниками Банку чи спеціалістами з обслуговування банкомату.
- Намагайтеся не тримати на виду Ваш гаманець та отримані з банкомату гроші. Не рахуйте отримані гроші, якщо біля банкомату присутні сторонні особи.
- Зберігайте видані банкоматом квитанції про проведені операції. Ви завжди можете запитати виписку про рух коштів безпосередньо в банкоматі. Це дозволить контролювати списання коштів з Вашого поточного рахунку.
- Пам'ятайте, якщо Ви не отримали кошти в банкоматі, хоча запит на це зробили, можливо, це - шахрайство, ознакою цього є наявність поблизу людини, що уважно спостерігає за Вашими діями, такі шахраї встановлюють пристрій - пастку, що

запобігає видачі платіжної картки або коштів Клієнту з подальшим їх присвоєнням шахраєм, у такому випадку, не відходячи від банкомату, зателефонуйте до Банку на номер **+38 (044) 279-51-61** та повідомте про можливе шахрайство.

Заходи безпеки при користуванні платіжною карткою в Інтернеті:

- Комп'ютерний вірус - комп'ютерна програма (шкідливий код), відмінною рисою якої є здатність збору інформації про дані платіжних карток (номер платіжної картки, CVV2 / CVC2, термін закінчення дії платіжної картки), які зберігаються / вводяться на комп'ютері, ноутбуці, планшеті, смартфоні, телефоні, зараженому вірусом.
- Переконайтеся, що в полі «Адреса» вибраного сайту вказана саме необхідна web-адреса, а не просто схожа на неї. При оплаті або введенні конфіденційної інформації про платіжну картку необхідно звернути увагу, щоб сайт був захищений: в адресному рядку браузера адреса обов'язково повинна починатися з https:// (а не просто http://), а у вікні браузера повинен з'явитися значок «закритий замочок -  ».
- Ніколи не вводьте PIN-код платіжної картки в Інтернеті. Ніколи не вводьте дані платіжної картки в спливаючих (pop-up) вікнах. Зверніть увагу, що для введення CVV2 / CVC2 на захищених сайтах використовується «віртуальна клавіатура», а на шахрайських та незахищених - ні.
- Уникайте проведення оплат за товари, послуги, комунальні платежі з публічного комп'ютера (кафе, бару, ресторану, готелю, бібліотеки, пошти, інших торговельно-сервісних підприємств, що надають послуги доступу до Інтернету), у разі, якщо цього не уникнути, вмикайте в браузері режим «приватного перегляду» (InPrivate Browsing).
- Не зберігайте на платіжній картці суми грошей більше, ніж потрібно для здійснення одноразового платежу в Інтернеті. Поповнюйте рахунок безпосередньо перед проведенням платежу, або блокуйте платіжну картку для онлайн-розрахунків і знімайте це обмеження перед процесом оплати. Ще один варіант - відкрити спеціальну платіжну картку для Інтернет-платежів, яку можна буде в разі необхідності поповнити з основної платіжної картки.
- Обов'язково встановіть на комп'ютері Firewall, ліцензійний антивірус, стежте за його своєчасним оновленням.
- Встановлюйте тільки ліцензійні операційні системи, своєчасно оновлюйте програмне забезпечення.
- Звертайте увагу на папки з випадковими іменами (що складаються з набору символів) в кореневих папках (диску С:), видаляйте їх, а також звертайте увагу на зайві файли при автозавантаженні, якщо Ви їх не обирали, видаляйте їх з вікна завантаження.
- Установіть ліміт на суми / кількість операцій для розрахунків у Інтернеті.

Заходи безпеки щодо ідентифікаційних даних:

Компрометація ідентифікаційних даних – це використання Вашого поточного рахунку в шахрайських цілях шахраєм, який володіє достатньою кількістю інформації про Вас, щоб відповісти на ідентифікаційні питання в телефонній розмові із співробітником Банку і отримати допуск до Вашого рахунку.

Шахрай, знаючи ідентифікаційну інформацію про Вас (контрольне кодове слово, номер паспорта, ІПН, дату народження, адресу проживання або прописки), може без Вашого відома:

- Змінити адресу проживання, а через деякий час повідомити, що платіжна картка загублена / вкрадена та замовити нову платіжну картку на іншу поштову адресу.

- Змінити контактний номер телефону і, таким чином, перенаправити СМС про проведення операцій платіжною карткою / ідентифікаційні дзвінки служби моніторингу, Контакт-центру Банку та інших підрозділів Банку на свій (мобільний) номер телефону.
- Збільшити / зняти авторизаційні ліміти на проведення операцій і зняти всі Ваші кошти або витратити їх на товари та послуги.
- Анулювати (зняти) лічильники неправильно введеного PIN-коду.

Де шахраї можуть отримати ваші ідентифікаційні дані:

- Інтернет: у соціальних мережах ВКонтакте, Однокласники, ВСети, Я.ру, Facebook, Google+, Tumblr, Twitter, Avaaz, Ask.fm, Badoo, Dudu, Flickr, Foursquare, Instagram, Last.fm, LinkedIn, LiveJournal, MySpace, Mixi, Orkut, Renren, Sina Weibo, SoundCloud, Tagged, відвідуючи відкриті сторінки та зламуючи закриті сторінки, Ваші електронні поштові скриньки, гаманці.
- Коли Ви передаєте персональні дані стороннім особам та організаціям у магазинах, на вулиці, приймаючи участь в акціях, розіграшах, отриманнях знижок (карток на знижки) на товари та послуги.
- В інших місцях, де Ви надаєте номер паспорта, ІПН, дату народження, адресу проживання або прописки.