ПАМ’ЯТКА

щодо здійснення безпечних онлайн-платежів

Для мінімізації ризиків втрат збережень з рахунків по Вашій платіжній картці (далі – картка) від неправомірних дій та намірів шахраїв і забезпечення секретності реквізитів власних карток, необхідно дотримуватися наступного:

Дозволяється повідомляти для переказу грошей:

- ✓ 16-значний номер Вашої картки;

Дозволяється повідомляти оператору контакт-центру при здійсненні вихідного дзвінка клієнтом Банку:

- ✓ П.І.Б. (за необхідності);
- ✓ Кодове слово для ідентифікації клієнта Банком / дівоче прізвище матері (оператор Контакт-центру може спитати його для проведення ідентифікації).

Не варто розголошувати третім особам реквізити та інші секретні дані Вашої картки:

- ✓ Термін дії картки;
- ✓ CVV2 / CVC2 (3-х значний код на звороті картки);
- ✓ PIN-код;
- ✓ 3D Secure (одноразовий короткостроковий пароль для підтвердження трансакції);
- ✓ не перетелефоновувати на ті номери, які тим чи іншим способом надійшли Вам через SMS-повідомлення чи в інших мессенджерах нібито від імені Банку із використанням подібного альфа-імені у стрічці з назвою контакту.

АТ «БАНК «ПОРТАЛ» може надсилати **SMS-повідомлення** виключно від власного зареєстрованого **альфа-імені «BANK PORTAL»** на фінансовий номер телефону клієнта, вказаний при укладанні з Банком договору банківського рахунку.

Для дистанційного обслуговування клієнтів Банку використовується Інтернет-банкінг **PORTAL.LINK** виключно з тієї URL-адреси, що міститься у цьому гіперпосиланні та через мобільний застосунок **PORTAL.LINK**, який можна завантажити з App Store та Play Market для зручного та безпечного використання власними фінансами.

Для безпечного здійснення онлайн-платежів, використовуючи систему дистанційного обслуговування різних Банків на території України та їх представництв на території інших країн, можна переглянути список їх на сторінці офіційного Інтернет-представництва Національного Банку України – список Банків та їх відокремлених підрозділів.

При підозрі щодо намірів та протиправних дій шахраїв відносно конфіденційних (секретних) даних з Вашою карткою, необхідно відразу звернутися до:

- ✓ контакт-центру Банку для блокування Вашої картки оператором контакт-центру за вищевказаними контактами або звернувшись безпосередньо до працівників Банку для встановлення лімітів на здійснення будь-яких трансакцій по картці у робочий час Банку;
- ✓ Департаменту кіберполіції онлайн за цим посиланням.

Рекомендуємо! Звернутися до мобільного оператора (віртуального мобільного оператора), якому Ви надаєте перевагу та користуєтесь його відповідними послугами, для відключення можливості віддаленого перевипуску SIM-картки (eSIM) для Вашого мобільного телефону, смартфону чи планшету.

Дізнатися про це та іншу необхідну інформацію можна зателефонувавши до контакт-центру Банку за номерами **0 800 50-24-50** або **+38 044 277-277-5**, які вказані на зворотній стороні кожної картки, виданої Банком.

Іншим корисним ресурсом для перевірки підозрілих сайтів є база шахрайських сайтів «BlackList EMA» та список надійних сервісів онлайн платежів і онлайн кредитування у «Білому списку». Для Вашої цікавості та обізнаності там можна пограти в онлайн-гру «ZДОЛАЙ ШАХРАЯ», в якій симулюються різні види платіжного шахрайства: телефонне, банкоматне та кредитне шахрайство, угон SIM-картки, шахрайство на дошках оголошень, фішинг, вішинг, шкідливе програмне забезпечення, програми-вимагачі тощо.

Перед здійсненням будь-яких онлайн-трансакцій слід переконатися в тому, що сайт не відноситься до **фішингових** та на безпечність з'єднання із ним разом із формою для заповнення реквізитів Вашої картки.

Ознаки **офіційного** та **безпечного** сайту:

- адреса сайту починається з https://… із наявним замочком ліворуч, що означає про те, що передача даних буде здійснюватися по захищеному каналу зв'язку та застосовується чинний SSL/TLS-сертифікат;
- сайт має бути зареєстрований на надійному домені, без використання конструкторів для створення сайтів, а в адресній стрічці мають відображатися різні адреси для різних сторінок сайту;
- відсутність помилок у структурі сайту, граматичних і синтаксичних помилок у його вмісті (контенту) чи сумнівного зовнішнього вигляду;
- легітимні сайти при введенні реквізитів платіжних карток у відповідні форми маскують їх зірочками або використовують віртуальну клавіатуру зі зміною її вигляду при введенні CVV2/CVC2 коду;

Фішингові сайти зазвичай існують короткий період часу та доволі часто після введення реквізитів картки відбувається збій операції або виникає невідома помилка.