**Рекомендації для клієнтів, які користуються**

**Мобільним додатком «Sportbank»**

1. Здійснюйте регулярні та своєчасні оновлення запропоновані Мобільним додатком;
2. Використовуйте надійні паролі для входу в Мобільний додаток;
3. Не розголошуйте і не передавайте свій логін, пароль, отп-коди отримані на фінансовий номер, третім особам (включаючи членів родини, друзів і т.д.);
4. Нікому не повідомляти і не передавати дані, які відображуються у Мобільному додатку;
5. Не зберігайте пароль у браузері, пароль необхідно вводити під час кожного нового сеансу роботи;
6. Не зберігайте пароль у вигляді простого тексту на комп’ютері, телефоні або у хмарі;
7. Для запобігання несанкціонованого доступу до конфіденційної інформації не повідомляйте свої авторизаційні дані;
8. Не відповідайте на запити, які містять вимогу надати або перевірити пароль тощо.
9. Не передавайте мобільний пристрій стороннім особам. Якщо Ваш смартфон потрапить до рук зловмисника, він зможе користуватися Мобільним додатком, отримувати одноразові паролі для входу та підтвердження платежів;
10. У разі втрати мобільного пристрою, негайно повідомте про це Банк. Якщо Ви загубили смартфон, терміново повідомте про це Банк, зателефонуйте до Контакт-центру і заблокуйте Ваші картки та номер телефону. Потім зв’яжіться з мобільним оператором для блокування SIM-картки;
11. Повідомляйте Банк про зміну фінансового номера телефону. Якщо у Вас змінився фінансовий номер телефону, обов’язково зверніться в Банк і попросіть змінити Ваш телефон у базі даних.
12. **Не рекомендується використовувати Мобільний додаток:**

* *в інтернет-кафе, публічних місцях, використовуючи публічні відкриті Wi-Fi-мережі, де немає гарантії того, що за вашими діями не стежить стороння людина;*
* *якщо Ви не впевнені в безпеці встановленого програмного забезпечення, а саме у відсутності вірусів, троянів, кейлоггерів – програм, що пересилають паролі користувача третім особам);*
* *на комп’ютерах, що перебувають у користуванні інших осіб (робочий комп’ютер на кілька користувачів, комп’ютер у бібліотеці, навчальному закладі, державній/приватній установі тощо);*
* *у місцях, де встановлені пристрої відеоспостереження, за допомогою яких можна отримати інформацію про ваші введені паролі.*

**11. Якщо вам надходять повідомлення з кодами для перереєстрації в Мобільному додатку або повідомлення для підтвердження операцій, які ви не виконували:**

* нікому не повідомляйте отримані дані (коди);
* негайно змініть пароль до Мобільного додатку;
* негайно заблокуйте платіжні картки засобами Мобільного додатку;
* перевірте в Мобільному додатку стан рахунків, у випадку виявлення розбіжностей – якомога швидше повідомте Банк про платежі, що ви не виконували;
* повідомте правоохоронні органи про факт несанкціонованого списання коштів з рахунку;
* дійте відповідно до подальших вказівок Банку та правоохоронних органів.

**Рекомендації щодо уникнення випадків підвищеного ризику збитків для користувача електронного платіжного засобу, в тому числі який доступний в Мобільному додатку «Sportbank»**

1. Встановіть ПІН-код/Пароль до Мобільного додатку і нікому їх не повідомляйте.
2. У випадку необхідності Ви можете змінити ПІН-код/ Пароль до Мобільного додатку самостійно з використанням засобів Мобільного додатку.
3. Ви повинні зберігати в таємниці ПІН-код/ Пароль до Мобільного додатку, CVV2/CVC2 та інформацію про Слово-пароль, інших даних Картки. Ви не повинні записувати ПІН-код на Платіжній картці або на інших предметах, які зберігаються разом з Карткою.
4. Ви повинні захищати ПІН-код/ Пароль до Мобільного додатку від «сторонніх очей» під час його введення.
5. Ви повинні користуватися карткою самостійно. Використання Картки в точці торгового еквайрингу або в пункті видачі готівки повинно проводитися в Вашій присутності. Нікому не передавайте Картку в користування (в т. ч. родичам). Використання Картки представником Клієнта за довіреністю заборонено.
6. Повідомляти Банк про будь-які підозри та сумніви, що стосуються Картки/ Мобільного додатку.
7. Не відключайте в Мобільному додатку функцію інформування про здійснення кожної операції з використанням Картки.
8. Регулярно формуйте виписку за опереціями засобами Мобільного додатку та перевіряйте їх на відповідність.
9. Не користуйтесь підозрілими банкоматами (на яких є предмети, залишки клею або інші сторонні пристрої, що викликають підозру).
10. Використовуйте сторінки в мережі Інтернет (сайти/портали) тільки відомих і перевірених Інтернет-магазинів.

**Рекомендації клієнтам щодо виявлення фішингових вебсайтів**

1. Перевірити сайт можна візуально, не використовуючи жодних додаткових сервісів: Якщо домен сторінки починається з http://, а не з https:// і не має стилізованого символа замка, який повідомляє про встановлення безпечного https-з'єднання, ресурс, як мінімум, небезпечний, як максимум – може бути фішинговим.

2. Реєстрація сайту, який надає послуги переказу коштів з картки на картку, а також поповнення мобільного телефону або онлайн-кредитування не в домені національного рівня «.UA», може бути ознакою фішингового ресурсу.

3. Наявність нульових комісій та інших «НЕЙМОВІРНИХ» пропозицій має насторожити.

4. Тематичні недоліки, наприклад відмінності в назві домену в адресному рядку і в тексті або на банері, теж можуть свідчити про те, що це шахрайський сайт.

5. Якщо в адресному рядку відображаються однакові адреси для всіх сторінок сайту, свідчить що це шахрайський сайт.

6. Легітимні сайти маскують введення карткових реквізитів (наприклад, зірочками) або використовують віртуальну клавіатуру, фішингові ресурси – не маскують.

7. При виявлені фішигових веб-сайтів необхідно про це повідомити технічну підтримки Банку за телефоном або через месенджери.

8. Для перевірки сайту, рекомендуемо скористатися базою шахрайських сайтів за посиланням.

9. З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб користуватись лише офіційним вебсайтом Банку <https://tascombank.ua/> або Лендинговим сайтом - [https://sportbank.com.ua](https://sportbank.com.ua/).

10. Довідник що містить інформацію про банки, що мають ліцензію та відокремлені підрозділи банків знаходиться на сайті Національного Банку України за [посиланням](https://bank.gov.ua/ua/supervision/institutions?page=1&perPage=5&search=&status=1&uid=&suid=&date_from=&date_to=&fb_date_from=&fb_date_to=)