

ПАМ'ЯТКА ДЕРЖАТЕЛЮ ПЛАТІЖНОЇ КАРТКИ

Шановний Клієнте,

Виконання даних рекомендацій допоможе мінімізувати ризик від шахрайських операцій при користуванні платіжною картою.

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ



Запам'ятайте Ваш ПІН-код та тримайте його в таємниці.



Зберігайте Ваш ПІН-код окремо від платіжної картки (далі- ПК) у не явному вигляді в недосяжному для третіх осіб місці. Не записуйте Ваш ПІН-код на ПК або на інших предметах, що, як правило, зберігаються разом із ПК.



Ніколи не розголошуйте та не повідомляйте персональні дані або інформацію про себе та реквізити ПК (номер, ПІН-код, CVV-код, термін дії) третім особам, у тому числі родичам, знайомим, працівникам Банку (або будь-якого іншого банку), які намагаються допомогти під час використання ПК.



Ніколи не передавайте у користування Вашу ПК та реквізити Вашої ПК третім особам, в тому числі через відкриті канали інформаційного обміну: електронну пошту, смс/push-інформування, соціальні мережі, чати, тощо.



Не відповідайте на електронні листи, телефонні дзвінки, смс, інші види запитів, у яких ніби від імені Банку пропонується надати Ваші персональні дані та/або реквізити Вашої ПК (такі листи в 90% випадків розсилаються шахраями та злоумисниками).



Пам'ятайте, що в разі розкриття Ваших персональних даних та/або реквізитів ПК (у тому числі ПІН-коду, CVV-коду), втрати ПК, існує ризик здійснення незаконних дій з коштами на Вашому рахунку з боку третіх осіб.



У разі, якщо Вашу ПК втрачено чи викрадено або з інших причин вона перестала функціонувати, якщо ПІН-код, та/або реквізити ПК стали відомі третім особам, негайно повідомте про це цілодобовий Контакт-центр Банку за телефоном: **0 800 30 88 80, +38 044 495 88 90**, або терміново зверніться до менеджера з обслуговування клієнтів у відділенні Банку.



Користуйтеся дистанційним банківським сервісом Winbank (далі – Winbank) та послугою смс/push- інформування щоб негайно дізнатись про всі операції з ПК.



Вживайте всі можливі заходи для запобігання втрати, крадіжки чи незаконному використанню ПК.

При користуванні Winbank:



Якщо при використанні Winbank виникли підозри на несанкціонований доступ до авторизаційних даних, та/або у разі втрати (крадіжки) авторизаційних даних, та/або у разі втрати номеру Вашого мобільного телефону або неможливості здійснення Вами контролю за своїм мобільним пристроєм, на який здійснюється відправлення одноразового цифрового паролю, та/або у разі виявлення випадків проведення по вашому рахунку операцій, що не були санкціоновані Вами, необхідно терміново припинити використання Winbank та негайно повідомити про інцидент Банк, звернувшись до цілодобового Контакт-центру Банку за телефоном: **0 800 30 88 80, +38 044 495 88 90**, або терміново зверніться до менеджера з обслуговування клієнтів у відділенні Банку.



У випадку, якщо пароль, або його частина стала відома третім особам, рекомендуємо негайно змінити пароль до Winbank.

При оплаті товарів та послуг, в тому числі в мережі Інтернет:



Додайте Вашу ПК до Google Pay або Apple Pay та розраховуйтеся телефоном – це зручно та безпечно.



Операції повинні проводитись в Вашій присутності. Не випускайте свою ПК з поля зору та ніколи не використовуйте ПІН-код при здійсненні оплати в мережі Інтернет.



Перед підтвердженням операції за допомогою ПК обов'язково перевірте суму, валюту платежу та дату операції.




З метою запобігання незаконним діям або сумнівним операціям з використанням даних ПК рекомендуємо для оплати товарів (послуг) встановити окремі граничні ліміти на операції в мережі Інтернет.



Рекомендуємо здійснювати оплати товарів (послуг) передбачених через мережу Інтернет тільки зі свого комп'ютеру/планшету/телефону з метою збереження конфіденційності персональних даних та/або інформації про картковий рахунок, та/або реквізитів ПК.



Обов'язково переконайтесь у безпечності web-сайту. Безпечні web-сайти відмічені значком у вигляді закритого замку  в адресному рядку браузера та адреса такого сайту має починатись з **https://**. Якщо в процесі використання платіжної картки Вами було виявлено фішингові web-сайти (веб ресурс, який виманює реквізити ПК під виглядом надання неіснуючих послуг, тощо) або отримано відомості подібного змісту просимо в найкоротший термін повідомити Банк найбільш зручним для Вас способом:

- звернувшись до цілодобового Контакт-центру Банку за телефоном: **0 800 30 88 80, +38 044 495 88 90**;
- електронним листом за адресою: info@piraeusbank.ua;
- за допомогою WEB дзвінка/або за допомогою опції "зворотній зв'язок" на Офіційному сайті Банку <https://piraeusbank.ua>
- звернувшись до менеджера з підтримки клієнтів у відділенні Банку.

При здійсненні операцій у банкоматі:



Вставляйте ПК в банкомат лише магнітною смугою донизу. Не застосовуйте фізичну силу, щоб вставити платіжну картку в отвір, призначений для приймання карток. Якщо ПК легко не вставляється, то не слід використовувати такий банкомат.



Рекомендуємо здійснення операцій з використанням ПК через банкомати, які встановлені в безпечних місцях (наприклад, у банках, установах та організаціях, великих торговельних комплексах, готелях, аеропортах тощо).



Не використовуйте пристрої, які потребують введення ПІН-коду для доступу в приміщення, де розташований банкомат.



Набирайте ПІН-код таким чином, щоб люди, які знаходяться у безпосередній близькості, не могли його бачити. При наборі ПІН-коду прикривайте клавіатуру рукою.



Не користуйтеся банкоматом, якщо на ньому явно видно сліди пошкодження або встановлення підозрілі пристрої.



Не користуйтеся банкоматом, якщо він знаходиться у погано освітлюваному та безлюдному місці.



Після отримання готівки в банкоматі необхідно її перерахувати. Переконайтесь у тому, що ПК була повернена банкоматом. Отримайте платіжну карту та чек (у разі його запиту). Лише після зазначених вище дій слід відходити від банкомата.



Якщо під час проведення операції із використанням банкомата ПК не повертається, то необхідно зателефонувати до банку за телефоном (який зазначено на банкоматі) та описати ситуацію, що склалася, а також звернутися з цього приводу до банку-емітента, який видав ПК для встановлення причин порушень та/або можливих технічних збоїв у роботі банкомата.

Будьте уважні та обережні!