Alliance bank

РЕКОМЕНДАЦІЇ ДЕРЖАТЕЛЯМ ПЛАТІЖНИХ КАРТОК ЩОДО ЇХ ВИКОРИСТАННЯ

Дотримання цих рекомендацій дасть змогу забезпечити держателям платіжних карток надійне їх зберігання, нерозголошення реквізитів платіжної картки, персонального ідентифікаційного номера (далі – ПІН) та інших даних, а також зменшить можливі ризики під час здійснення операцій з використанням платіжної картки в банкоматах, безготівкової оплати товарів і послуг, у тому числі через мережу Інтернет. Рекомендації діють в частині що не суперечать правилам користування платіжною карткою відповідної платіжної системи (у разі її надання емітентом держателю). Ці рекомендації не поширюються на платіжні картки Національної системи масових електронних платежів.

Загальні рекомендації

1. Під час отримання платіжної картки в банку перевірте особисті дані, термін дії, цілісність конверта (якщо він є) з персональним ідентифікаційним номером (далі – ПІН).
2. Поставте власний підпис на зворотному боці платіжної картки (на спеціально відведеній смузі, що призначена для підпису держателя). Це зменшить вірогідність використання платіжної картки без вашої згоди або в разі її втрати.
3. Будьте уважні до умов зберігання та використання платіжної картки. Не піддавайте платіжну картку механічним, температурним та електромагнітним діям, а також уникайте потрапляння на неї вологи. Платіжну картку не можна зберігати разом з мобільним телефоном, побутовою та офісною технікою, а також поблизу металевих предметів та інших магнітних носіїв/пристроїв
4. Банк-емітент ніколи не здійснює запити та/або телефонні дзвінки своїм клієнтам – держателям платіжних карток щодо перевірки реквізитів виданої платіжної картки або уточнення персональних даних (серія, номер паспорта, ідентифікаційний номер, персональний пароль, номер мобільного телефону тощо).
5. У жодному випадку не розголошуйте номер картки, ПІН та CVV-код стороннім особам (у тому числі родичам, знайомим, дітям, працівникам банку, касирам та особам, які намагаються допомогти вам під час використання платіжної картки).
6. Запам’ятайте ПІН та зберігайте його окремо від платіжної картки та гаманця в недоступному для сторонніх осіб місці.
7. Не зберігайте ПІН на смартфоні та планшеті.
8. Не слід передавати платіжну картку іншим особам (у тому числі родичам). Персоніфіковану платіжну картку (що містить прізвище та ім’я фізичної особи) має право використовувати виключно та фізична особа, яка її отримала.
9. Не розголошуйте та не повідомляйте реквізити платіжної картки (номер, ПІН, CVV-код, термін дії), власні персональні дані або будь-яку іншу інформацію, що стосується платіжної картки на вимогу сторонніх осіб (у тому числі й працівників банку). У разі виникнення такої ситуації одразу телефонуйте до банку, який видав платіжну картку, і повідомте про цей факт (телефон банку, контакт-центру банку чи служби клієнтської підтримки зазначено на зворотному боці платіжної картки).
10. Використовуйте різні паролі для кожного важливого облікового запису, наприклад, для особистого кабінету, електронної пошти й інтернет-банкінгу. Використовувати ті самі паролі небезпечно. Якщо хтось дізнається пароль для одного облікового запису, то зможе отримати доступ до вашої електронної пошти, адреси та навіть грошей.Не можна використовувати паролі, які легко вгадати, наприклад, "Qwerty123", використовувалися раніше для облікового запису, починаються або закінчуються пробілом.

Пароль має містити принаймні 8 символів. Це можуть бути комбінації літер, цифр і символів. Надійний пароль допомагає захистити: особисту інформацію, електронні листи, файли, обліковий запис від зламу.

11. Ніколи не передавайте реквізити платіжної картки через відкриті канали інформаційного обміну: електронну пошту, смс, соціальні мережі, чати тощо.
12. Зауважимо, що доцільно мати при собі номер платіжної картки та контактні телефони банкуемітента на інших носіях інформації (у записнику, мобільному телефоні, персональному комп'ютері тощо), але в жодному випадку не разом із записом про ПІН.
13. Доцільно встановити добовий ліміт на суму та кількість операцій із застосуванням платіжної картки та підключити електронну послугу оповіщення про проведені операції (наприклад, у вигляді коротких текстових повідомлень на мобільний телефон (смс), засобами електронної пошти або в інший спосіб) з метою запобігання незаконним діям/сумнівним операціям з використанням платіжної картки (та/або її реквізитів) та зняття коштів з вашого карткового рахунку.
14. Не слід відповідати на електронні листи, телефонні дзвінки та смс у яких ніби від імені банку пропонується надати персональні дані (такі листи в 90% випадків розсилаються шахраями та зловмисниками).
15. Не слід відкривати посилання (сторінки/сайти/портали тощо) у мережі Інтернет, зазначені в таких "листах-розсилках" (у тому числі включаючи офіційну сторінку банку), оскільки це можуть бути підробні (сторінки-двійники), через які можуть здійснюватися незаконні дії/сумнівні операції з використанням даних вашої платіжної картки.
16. Для забезпечення безпеки та в цілях інформаційної взаємодії з банком-емітентом рекомендуємо використовувати виключно ті реквізити засобів зв'язку [мобільних, стаціонарних телефонів, факсів, сторінок у мережі Інтернет (сайтів/порталів), пошти/електронної пошти тощо], які зазначені в документах, отриманих безпосередньо в банку-емітенті.
17. У разі втрати платіжної картки держатель повинен негайно повідомити про це банк-емітент. Емітент не несе відповідальності за переказ коштів за допомогою такої платіжної картки, ініційований до отримання відповідного повідомлення, якщо інше не передбачено договором.
18. Запам'ятайте, що розголошення ПІН, персональних даних, реквізитів платіжної картки чи її втрата суттєво підвищує ризик здійснення незаконних дій з боку третіх осіб та сприяє зникненню коштів з Вашого рахунку.
19. Взаємовідносини банка та клієнта за операціями з використанням платіжних карток установлюються укладеним між ними договором.
20. Держатель платіжної картки повинен самостійно та постійно контролювати стан свого банківського рахунку та відстежувати рух коштів за всіма операціями, які він здійснював.
21. Рекомендуємо щомісяця отримувати від банку (у будь-який зручний спосіб: поштою, засобами електронної пошти, факсом тощо) виписку за Вашим рахунком.
22. Перед тим, як поїхати закордон, перевірте термін дії картки та переконайтеся, що у Вас достатньо коштів на рахунку. Також доцільно переконатись, що всі Ваші обов'язкові платежі за річне обслуговування зроблені вчасно. У разі потреби – поповніть картковий рахунок.
23. У країнах із високим ризиком шахрайства банком-емітентом можуть бути встановлені додаткові обмеження на проведення операцій із використанням платіжних карток. Тож, якщо Ви плануєте подорож до однієї з таких країн – зверніться до банку-емітента для зняття обмежень на використання Вашої платіжної картки або встановлення інших добових лімітів.
24. Ваші рахунки в банку прив'язані до номеру вашого мобільного телефону (фінансового номеру). Отримавши доступ до SIM-карти, шахраї можуть отримати доступ і до рахунків.
    Якщо ваш номер припинив відповідати – негайно повідомте про це свій банк та блокуйте свої картки. Після цього зверніться до мобільного оператора про блокування номеру та перевипуску SIM-картки.

Здійснення операцій через банкомат

1. Рекомендуємо здійснювати операції з використанням платіжних карток через банкомати, які встановлені в безпечних місцях (наприклад, в установах, банках, великих торговельних комплексах, готелях, аеропортах тощо).
2. Не використовуйте пристрої, які потребують уведення ПІН для доступу в приміщення, де розташовано банкомат.
3. Перед використанням банкомата огляньте його щодо наявності додаткових приладів, які не відповідають його конструкції та розташовані в місці набору ПІНу, та в місці (отвір), призначеному для приймання карток (наприклад, наявність нерівно встановленої клавіатури для набору ПІН). У разі виявлення зазначеного не використовуйте такий банкомат.
4. Якщо клавіатура або місце для приймання карток банкомата обладнані додатковими пристроями, що не відповідають його конструкції, не використовуйте його для здійснення операцій з використанням платіжної картки і повідомте про це банк за номером телефону, який зазначено на банкоматі.
5. Не застосовуйте фізичну силу, щоб вставити платіжну картку в отвір призначений для приймання карток. Якщо платіжна картка легко не вставляється, то не використовуйте такий банкомат.
6. Набирайте ПІН таким чином, щоб особи, які перебувають поруч, не змогли його побачити. Під час набору ПІНу прикривайте клавіатуру рукою.
7. Якщо банкомат працює некоректно (наприклад, довгий час перебуває в режимі очікування, мимоволі перезавантажується), відмовтесь від послуг такого банкомата, відмініть поточну операцію, натиснувши на клавіатурі кнопку ”Відміна” (”Отмена” чи ”CANCEL”) і дочекайтесь повернення платіжної картки.
8. Після отримання готівки в банкоматі необхідно її перерахувати та переконатись у тому, що платіжна картка була повернена банкоматом, дочекатись видачі чека в разі його запиту і тільки після цього відходити від банкомата.
9. Роздруковані банкоматом чеки потрібно зберігати для звірки зазначених у них сум з випискою про рух коштів на картковому рахунку.
10. Не слід проводити ніяких дій за підказками третіх осіб, а також не приймайте від них допомоги під час здійснення операцій через банкомат з використанням платіжної картки.
11. Якщо під час проведення операції через банкомат платіжна картка 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 платіжну картку.
12. Не здійснюйте операцій через банкомат/термінал самообслуговування, якщо Вам не зрозуміле його меню або інформація на екрані. Також не слід використовувати банкомати та термінали, якщо на них містяться невідомі пристрої та ті, що розташовані в підозрілих неосвітлених місцях.

Здійснення безготівкових розрахунків

1. Будьте уважні, не поспішайте. Відповідайте за власні дії. Не вимагайте від торговця/продавця/касира/оператора здійснити операцію за картками сторонніх осіб (зокрема за карткою чоловіка/дружини/батьків/дітей тощо). У такий спосіб Вас можуть запідозрити як шахрая (зловмисника) та направити до Вас працівників служби безпеки торговельно-сервісного підприємства або поінформувати банк чи правоохоронні органи.
2. Забороняється під час здійснення безготівкових розрахунків передавати платіжну картку або чек для підпису третім особам чи неповнолітнім дітям.
3. Не використовуйте платіжну картку в торговельній мережі для оплати товарів або послуг, якщо торговець/продавець/касир (у ресторані, магазині, на АЗС тощо) викликав у вас недовіру.
4. Розрахунки з використанням платіжної картки мають виконуватися тільки у вашій присутності. Це забезпечить зниження ризику неправомірного отримання ваших персональних даних, зазначених на платіжній картці.

5. Під час використання платіжної картки для оплати товарів або послуг продавець/касир може вимагати від держателя платіжної картки надати паспорт, підписати квитанцію або ввести ПІН. Перед набором ПІНу слід переконатися, що треті особи, які перебувають у безпосередній близькості від вас, не зможуть його побачити. Перед тим, як підписати квитанцію, в обов'язковому порядку перевірте суму, що зазначена на ній.
6. Перед набором ПІН слід переконатися, що треті особи, які перебувають у безпосередній близькості, не зможуть його побачити.
7. Перед тим, як підписати квитанцію, в обов'язковому порядку перевірте суму, зазначену на ній.
8. Якщо під час спроби здійснити оплату товарів або послуг з використанням платіжної картки не вдалося здійснити успішно операцію, то необхідно зберігати один примірник виданої терміналом квитанції для перевірки відсутності зазначеної операції у виписці про рух коштів за картковим рахунком.
9. У випадках вилучення платіжної картки третіми особами відповідно до законодавства України, вимагайте у особи, що вилучає платіжну картку, розписку про її вилучення.
10. Пам'ятайте, що платіжна картка – як готівка. Не залишайте її без нагляду.

Виконання операцій через мережу Інтернет

1. Не використовуйте ПІН під час замовлення товарів або послуг через мережу Інтернет, а також за телефоном/факсом.
2. Не повідомляйте інформацію про платіжну картку або картковий рахунок через мережу Інтернет, наприклад ПІН, паролі доступу до рахунків, термін дії платіжної картки, кредитні ліміти, персональні дані тощо.
3. З метою запобігання незаконним діям або сумнівним операціям з використанням даних платіжної картки міжнародної платіжної системи рекомендуємо для оплати товарів (послуг) через мережу Інтернет використовувати окрему платіжну картку (так звана "віртуальна картка") з граничним лімітом, яка передбачена тільки для цієї цілі та яка не дає змоги здійснювати з її використанням операції в торговельній мережі та зняття готівки.
4. Необхідно використовувати сторінки в мережі Інтернет (сайти/портали) тільки відомих і перевірених Інтернет-магазинів.
5. Рекомендуємо не сканувати QR-коди на сторінках/сайтах, що викликають підозру.
6. Не слід використовувати систему Інтернет-банкінг через публічні мережі Wi-Fi (насамперед у кафе, барах, ресторанах, парках, готелях тощо).
7. Обов'язково переконайтесь у правильності зазначення адреси сторінок у мережі Інтернет (сайтів/порталів), до яких підключаєтесь і через які збираєтеся здійснювати оплату товарів (послуг), оскільки схожі адреси можуть використовуватися для здійснення незаконних дій або сумнівних операцій з використанням персональних даних платіжної картки.
8. Рекомендуємо здійснювати оплату товарів (послуг), придбаних через мережу Інтернет, тільки зі свого комп'ютера з метою збереження конфіденційності персональних даних та/або інформації про картковий рахунок. Якщо оплата товару (послуги) здійснюється через чужий комп'ютер, рекомендуємо після завершення всіх розрахунків переконатися, що персональні дані та інша інформація не збереглася (знову відкривши сторінку продавця, на якій здійснювалась оплата товару).
9. Якщо оплата товару (послуги) здійснюється через чужий комп'ютер, то рекомендуємо після завершення всіх розрахунків переконатися, що персональні дані та інша інформація не збереглася (знову відкривши сторінку продавця, на якій здійснювалась оплата товару).
10. Слід встановити на свій комп'ютер антивірусне програмне забезпечення і регулярно здійснювати його оновлення та оновлення інших програмних продуктів (операційної системи, прикладних програм). Це захистить вас від проникнення неліцензійного програмного забезпечення (вірусів).

11. Перевірити сайт можна за допомогою спеціального сервісу Кіберполіції: https://cyberpolice.gov.ua/stopfraud/ або сервісу Асоціації "ЄМА" - https://www.ema.com.ua/blacklist/
12. Випадково розкрили дані платіжної картки на підозрілому сайті - негайно дзвоніть на гарячу лінію Банку 0800 60 2222 (безкоштовно по Україні).
13. Якщо ви зрозуміли, що потрапили в руки шахраям через фішинговий сайт – повідомте про це Кіберполіцію.
14. Заяву в Кіберполіцію можна лишити тут - https://ticket.cyberpolice.gov.ua/ або зателефонувавши за номером - 0 800 505 170.

Закриття карткового рахунку

1. Пам'ятайте, що поточні/карткові рахунки закриваються на підставі заяви клієнта, якщо інше не передбачено договором.
2. У разі звільнення з роботи або дострокового розірвання договору з вашої ініціативи, якщо ви не плануєте використовувати в подальшому рахунок та якщо банком передбачено стягнення комісійної винагороди за його обслуговування, доцільно закрити поточний/картковий рахунок, який був відкритий вам для отримання заробітної плати. Для цього ви маєте звернутись із заявою про закриття рахунку до банку, якщо інше не передбачено договором, і повернути платіжну картку (у разі потреби), одержати виписку про рух коштів за картковим рахунком.
3. Під час закриття карткового рахунку (після виконання зобов'язань або в разі розірвання чи закінчення терміну дії договору) банк зобов'язаний видати залишок коштів (у разі його наявності) та на вимогу держателя платіжної картки – довідку про закриття рахунку та повернення платіжної картки, кредиту і процентів за ним. Кошти видаються готівкою або за дорученням клієнта перераховуються на інший рахунок
4. Нагадуємо, що банком (відповідно до умов укладеного договору та затверджених тарифів) утримується/стягується плата за: обслуговування рахунку. Тож, якщо Ви вирішили закрити рахунок і повернути платіжну картку до банку-емітента, то не слід зволікати і залишати це "на потім". Це убезпечить Вас від зайвих витрат та боргів перед банком
5. Не рекомендуємо власноруч знищувати платіжну картку (навіть якщо рахунок у банку вже закрито). Це повинні робити (бажано у Вашій присутності) відповідальні працівники банкуемітента.

Більше інформації читай на #ШахрайГудбай за посиланням https://bank.gov.ua/promo/stopfraud/
Потрапив в руки шахрая?
Телефонуй в Кіберполіцію – 0 800 505 170 або звернись онлайн за посиланням https://cyberpolice.gov.ua/