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. Ніколи не розголошуйте ПІН стороннім особам, у тому числі родичам, знайомим, працівникам банку, касирам та особам, які намагаються допомогти вам під час використання платіжної картки.
2. ПІН необхідно запам’ятати або зберігати його окремо від платіжної картки в недоступному для сторонніх осіб, у тому числі родичів, місці.
3. Ніколи не передавайте платіжну картку для використання іншими особами, у тому числі родичами. Якщо на платіжній картці нанесено прізвище та ім’я фізичної особи, то тільки ця фізична особа має право використовувати платіжну картку.
4. Не розголошуйте та не повідомляйте персональні дані або інформацію про платіжну картку (у тому числі ПІН) на вимогу будь-яких сторонніх осіб, у тому числі й працівників банку. У разі виникнення такої ситуації зателефонуйте до банку-емітента, який видав платіжну картку, і повідомте про цей факт.
5. Під час отримання платіжної картки поставте підпис на її зворотному боці в місці, яке призначено для підпису держателя платіжної картки. Це зменшить ризик використання платіжної картки без вашої згоди в разі її втрати.
6. 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.
7. Телефон банку-емітента, який видав платіжну картку, зазначено на 2 зворотному боці платіжної картки. Також потрібно завжди мати при собі контактні телефони банку-емітента, номер платіжної картки на інших носіях інформації: у записнику, мобільному телефоні тощо, але не разом із записом про ПІН.

8. З метою запобігання незаконним операціям з використанням платіжної картки та зняття коштів з вашого карткового рахунку доцільно встановити добовий ліміт на суму та кількість операцій із застосуванням платіжної картки та одночасно підключити електронну послугу оповіщення про проведені операції (наприклад, оповіщення у вигляді коротких текстових повідомлень на мобільний телефон (SMS) або іншим способом).
9. Не рекомендується відповідати на електронні листи, у яких від імені банку пропонується надати персональні дані. Не потрібно відкривати сторінки в мережі Інтернет (сайти/портали), що зазначені в листах (уключаючи офіційну сторінку банку в мережі Інтернет), оскільки це можуть бути сторінки-двійники, через які можуть здійснюватися незаконні дії/сумнівні операції з використанням даних вашої платіжної картки.
10. У цілях інформаційної взаємодії з банком-емітентом рекомендуємо використовувати тільки реквізити засобів зв'язку (мобільних, стаціонарних телефонів, факсів, інтерактивних сторінок у мережі Інтернет (сайтів/порталів), звичайної та електронної пошти тощо), які зазначені в документах, отриманих безпосередньо в банку-емітенті.
11. Пам'ятайте, що в разі розкриття ПІНу, персональних даних, втрати платіжної картки існує ризик здійснення незаконних дій з коштами на вашому рахунку з боку третіх осіб.

У разі втрати платіжної картки держатель повинен негайно повідомити про це емітента. У противному разі емітент не несе відповідальності за переказ коштів, ініційований до отримання такого повідомлення за допомогою цієї платіжної картки, якщо інше не передбачено договором.

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.

Здійснення безготівкових розрахунків

1. 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.
2. Розрахунки з використанням платіжної картки мають виконуватися тільки у вашій присутності. Це забезпечить зниження ризику неправомірного отримання ваших персональних даних, зазначених на платіжній картці.
3. 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.
4. 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.

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. 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.
6. 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).
7. 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).

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.

РЕКОМЕНДАЦІЇ КЛІЄНТАМ ЩОДО ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБСАЙТІВ

Фішинг – це схема, застосування якої змушує користувачів передавати конфіденційну інформацію шахраям для наступного використання такої інформації у зловмисних цілях.

Конфіденційною інформацією є наступна інформація:
- логін та пароль для входу в систему Інтернет-Банкінг;
- номер, термін дії, CVV2/CVC2, ПІН платіжної картки;
- одноразові паролі підтвердження операцій;
- адреса вашої електронної пошти;
- фінансовий номер вашого телефону;
- слово-пароль до картки, відповіді на секретні питання тощо.

Основні схеми фішингових операцій:
1. використання розсилок електронних листів (СПАМу) з певними пропозиціями купівлі товарів та послуг, листами-повідомленнями про блокування облікового запису пошти, доступу до системи клієнта банку та ін.;
2. переадресування користувачів на зловмисні (підробні) сайти, які ззовні, або за доменним ім’ям, схожі до офіційних сайтів певних організацій;
3. голосовий фішинг;
4. фішингові СМС – повідомлення;
5. фішинг в соціальних мережах тощо.

Приклад: отримавши незаконним, або підступним (обман) шляхом інформацію про номер платіжної картки, термін дії, ім’я та прізвище держателя платіжної карти, CVV/CVC2-код – злочинці можуть використати дану інформацію для здійснення несанкціонованих списань грошових коштів з даної платіжної карти. Держатель платіжної картки дізнається про такі операції вже за фактом їх здійснення, шляхом отримання інформації про рух коштів за допомогою СМС-повідомлення від банку, або переглянувши інформацію про рух коштів в системі Інтернет-Банкінгу.

Для забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб під час роботи з сайтом ПуАТ КБ «АКОРДБАНК» (далі – Банк) для клієнтів Банку пропонуємо використовувати рекомендації наведені нижче:
1. Користуйтесь лише офіційним сайтом Банку за посиланням: https://accordbank.com.ua/
2. Якщо Вас було переадресовано на невідомий сайт, з незнайомим, або іншим доменним іменем - не вводьте конфіденційну інформацію ні в які запропоновані поля.

УВАГА! Представники банку за жодних обставин не здійснюють телефонні дзвінки своїм діючим та потенційним клієнтам для отримання будь-якої конфіденційної інформації.