ПАМЯТКА
О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ПЛАТЕЖНЫХ КАРТ
АО «НДБанк»

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность платежной карты, ее реквизитов, ПИН и других данных, а также снизит возможные риски при совершении операций с использованием платежной карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Общие рекомендации

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании платежной карты.
2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от платежной карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.
3. Никогда ни при каких обстоятельствах не передавайте платежную карту для использования третьим лицам, в том числе родственникам. Если на платежной карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать платежную карту.
4. При получении платежной карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя платежной карты, если это предусмотрено. Это снизит риск использования платежной карты без Вашего согласия в случае ее утраты.
5. Будьте внимательны к условиям хранения и использования платежной карты. Не подвергайте платежную карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Платежную карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
6. Телефон кредитной организации - эмитента платежной карты (кредитной организации, выдавшей платежную карту) указан на оборотной стороне платежной карты. Также необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента платежной карты и номер платежной карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.
7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по платежной карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).
8. При получении просьбы, в том числе со стороны сотрудника кредитной организации, сообщить персональные данные или информацию о платежной карте (в том числе ПИН) не сообщайте их. Перезвоните в кредитную организацию - эмитент платежной карты (кредитную организацию, выдавшую платежную карту) и сообщите о данном факте.
9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента платежной карты (кредитной организации, выдавшей платежную карту)) предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
10. В целях информационного взаимодействия с кредитной организацией - эмитентом платежной карты (кредитной организации, выдавшей платежную карту) рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в кредитной организации - эмитенте платежной карты.

11. Помните, что в случае раскрытия ПИН, персональных данных, утраты платежной карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если платежная карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент платежной карты (кредитную организацию, выдавшую платежную карту) и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент платежной карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией - эмитентом платежной карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей платежной карты до момента уведомления об этом кредитной организации - эмитента платежной карты, не возмещаются.

Рекомендации при совершении операций с платежной картой в банкомате

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.

3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.

5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования платежной карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

6. Не применяйте физическую силу, чтобы вставить платежную карту в банкомат. Если платежная карта не вставляется, воздержитесь от использования такого банкомата.

7. Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.

8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку "Отмена", и дождаться возврата платежной карты.

9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что платежная карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.

11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с платежной картой в банкоматах.

12. Если при проведении операций с платежной картой в банкомате банкомат не возвращает платежную карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент платежной карты (кредитную организацию, выдавшую платежную карту),

которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

Рекомендации при использовании платежной карты для безналичной оплаты товаров и услуг

1. Не используйте платежные карты в организациях торговли и услуг, не вызывающих доверия.

2. Требуйте проведения операций с платежной картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на платежной карте.

3. При использовании платежной карты для оплаты товаров и услуг кассир может потребовать от владельца платежной карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.

4. В случае если при попытке оплаты платежной картой имела место "неуспешная" операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

Рекомендации при совершении операций с платежной картой через сеть Интернет

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

2. Не сообщайте персональные данные или информацию о платежной(ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия платежной карты, кредитные лимиты, историю операций, персональные данные.

3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную платежную карту (так называемую виртуальную карту) с предельным лимитом, предназначенную только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

6. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о платежной(ом) карте (счете).

В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

7. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление и обновление других используемых Вами программных продуктов (операционной системы и прикладных программ), это может защитить Вас от проникновения вредоносного программного обеспечения.

Возможные виды мошенничества

Фишинг

Рассылка пользователям сети Интернет электронных писем от имени банка-эмитента, с просьбой уточнить данные по платежным картам, либо содержащие ссылку на сайт банка, который держателю карты необходимо посетить. На сайте предлагается ввести личные данные, якобы потерянные из-за технического сбоя системы: номер платежной карты, идентификатор, пароль и иногда даже Пин-код. После этого финансовые средства с карт-счетов могут использоваться мошенниками через интернет-магазины.

Скимминг

Существуют специальные виды электронных устройств, которые при установке на банкоматах позволяют считывать и фиксировать как реквизиты карты (номер карты, специальные параметры), так и Пин-код. Подобные устройства хитро замаскированы под обычные части банкомата. Считывающее устройство накладывается поверх гнезда для ввода карточки, поверх клавиатуры или используются миниатюрные видеокамеры, замаскированные под ящичек с информационными/рекламными брошюрами.

Важно!

Настоящий сотрудник банка никогда не просит информацию из SMS- и/или PUSH-уведомлений, такую как коды доступа в личный кабинет и коды подтверждения операций, а также CVV/CVC-коды на обратной стороне карты.

При выявлении Банком в момент исполнении распоряжения Клиента признаков, которые могут указывать на то, что перевод осуществляется без добровольного согласия Клиента, Банк с целью снижения таких рисков приостанавливает исполнение распоряжения Клиента сроком на два дня, а в случае осуществления перевода денежных средств с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России, отказывает в совершении соответствующей операции (перевода).

В день приостановления распоряжения Банк информирует Клиента по доступным каналам связи, указанным в Договорах/Заявлениях, подписанных с Банком, о причине приостановления приема распоряжения к исполнению и необходимости предоставления подтверждения данного распоряжения не позднее одного дня, следующего за днем приостановления Банком.

Клиент должен подтвердить Банку и (или) предоставить запрашиваемую Банком информацию, что перевод денежных средств не является переводом денежных средств без добровольного согласия Клиента по доступным каналам связи, указанным в Договорах/Заявлениях, подписанных с Банком.

В случае отказа Банка по переводу денежных средств в совершении Клиентом операций с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России Банк информирует Клиента по доступным каналам связи, указанным в Договорах/Заявлениях, подписанных с Банком, о возможности совершения Клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода (далее – повторная операция).

При получении от Клиента подтверждения о действительности распоряжения и в случае осуществления действий по совершению Клиентом повторной операции Банк принимает к исполнению подтвержденное распоряжение Клиента или совершает повторную операцию, но при

отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение Клиента к исполнению.

При неполучении от Клиента подтверждения распоряжения и (или) информации, запрошенной Банком, указанное распоряжение считается не принятым к исполнению.

Клиент для снижения рисков обязан ознакомиться с признаками осуществления переводов денежных средств без добровольного согласия, которые установлены Банком России и размещены на его официальном сайте в информационно-телекоммуникационной сети «Интернет».

Что делать в экстренных случаях

- Внимательно отнеситесь к звонкам от тех, кто представляется сотрудником банка или полиции. Помните, что **служба безопасности Банка не звонит Клиентам** для выяснения реквизитов карты, паролей для доступа в интернет-банк и кодов для подтверждения операций.

- Если вы подозреваете, что к вам обратились мошенники и им стали известны важные данные, **немедленно позвоните в контакт-центр АО «НДБанк» по телефону:**
  +7(495) 899 36 33.
  Для удобства заранее сохраните наш номер в своей телефонной книге.

- Если вы получили sms об операции, которую не совершали, обратитесь в банк по телефону +7(495) 899 36 33.

- **Заблокируйте карту**, если она была потеряна или забыта в банкомате. Для блокировки карты обратитесь в круглосуточный контакт-центр по телефону +7(495) 899 36 33.
  Даже при заблокированной карте вы можете снять наличные в отделении Банка при наличии паспорта.