Памятка «Правила безопасного использования карт Почта Банка»

Термины, указанные в настоящей памятке с заглавной буквы, имеют то же значение, что и в договоре о выпуске и обслуживании банковской карты (если иное прямо не определено непосредственно в тексте настоящей памятки).

Поздравляем! Вы стали держателем банковский карты, выпущенной ПАО «Почта Банк» (далее – Банк).

Выполнение несложных рекомендаций из настоящей памятки позволит вам сохранить банковскую карту и значительно уменьшить риск потери ваших денег при использовании банковской карты в банкоматах, магазинах и в сети Интернет. Настоящая памятка описывает порядок и правила пользования банковской картой, включая ограничения способов и мест её использования, случаи повышенного риска использования банковской карты.

Памятка размещается на сайте Банка в сети Интернет по адресу: www.pochtabank.ru, а также может быть размещена в иных открытых источниках (по выбору Банка).

1. ОБЩИЕ РЕКОМЕНДАЦИИ

1.1. Запишите и храните под рукой контактный телефон Банка (он указан в договоре о выпуске и обслуживании банковской карты, на оборотной стороне карты, выпущенной на материальном носителе, на сайте Банка, в системе дистанционного банковского обслуживания Почта Банк Онлайн, в иных официальных и достоверных источниках). Так вы всегда сможете позвонить в Банк и получить нужную вам консультацию, а при необходимости – заблокировать утерянную или украденную у вас карту.

1.2. Никогда и никому не сообщайте ПИН карты – ни родственникам, ни знакомым, ни сотрудникам Банка, ни кассирам. Если кто-либо просит вас сообщить ваши персональные данные, информацию о вашей карте или ПИН - откажите. При малейшем сомнении позвоните в Банк и сообщите о такой просьбе.

1.3. При вводе ПИН избегайте присутствия посторонних и никогда не прибегайте к их помощи.

1.4. Не храните ПИН вместе с картой. Не записывайте его на лицевой или оборотной стороне карты. Не используйте для его хранения память вашего мобильного устройства или компьютера. Если запомнить ПИН затруднительно, запишите его в неявном виде и храните в недоступном для других лиц месте.

1.5. Никогда и никому не передавайте карту для использования. Картой можете пользоваться только вы сами.

1.6. Никому не сообщайте (в т.ч. сотрудникам Банка) код CVV / CVC / ППК2, номер карты и другие реквизиты карты, а также полученные от Банка одноразовые пароли.

1.7. Будьте внимательны, Банк направляет вам через систему дистанционного банковского обслуживания Почта Банк Онлайн информацию о каждой совершенной по карте операции. Если вы получили такую информацию и знаете, что не совершали указанной операции, срочно позвоните в Банк и сообщите о произошедшем. Карта будет заблокирована, и вы сохраните свои деньги.

1.8. При получении карты на материальном носителе распишитесь на ее оборотной стороне, в предназначенном для этого месте. Это снизит риск использования карты другими лицами без вашего согласия.

1.9. Не храните карту на материальном носителе рядом с мобильными устройствами, бытовой и офисной техникой.

1.10. Не отвечайте на электронные письма, в которых от имени Банка или его представителей запрашиваются ваши персональные данные, пароли, ПИН. Не переходите по ссылкам, указанным в таких письмах, включая ссылки на сайт Банка. Переход по таким ссылкам может привести к потере ваших денег.

1.11. Если вы предполагаете, что информация о вашей карте или ПИН стала известна другим лицам, или если ваша карта была украдена или утрачена, незамедлительно позвоните в Банк и сообщите о случившемся. Следуйте указаниям сотрудника Банка. Помните, до момента обращения в Банк риск несанкционированного списания ваших денег несете вы сами.

1.12. Если вам поступило сообщение (или телефонный звонок) с неизвестного вам номера о блокировке или необходимости срочного перевыпуска вашей карты с просьбой перезвонить по указанному в сообщении (или сообщенному при разговоре) номеру телефона, – ни в коем случае не перезванивайте и не отправляйте никаких сообщений на этот номер. Позвоните в Банк по телефонам, которые известны вам из официальных и достоверных источников либо обратитесь в Банк лично.

1.13. Дополнительно, для снижения риска несанкционированного использования карты (реквизитов карты) третьими лицами при компрометации, а также при утере/краже/изъятии карты (реквизитов карты), установите лимиты на проведение операций (в месяц / в день / на каждую операцию), либо отключите возможность совершения операций:
- через сеть Интернет;
- за пределами территории Российской Федерации;
- по получению наличных денежных средств в банкоматах;
- по переводу денежных средств на карты других банков посредством сервиса по переводу денежных средств с использованием реквизитов банковских карт.

1.13.1. При временном прекращении использования карты в целях безопасности - отключите возможность проведения любых расходных операций с использованием данной карты.

1.14. Для установления лимита на проведение операций или отключения возможности проведения операций необходимо направить в Банк через каналы Почта Банк Онлайн соответствующий запрос.

2. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ КАРТ В БАНКОМАТЕ / ТЕРМИНАЛЕ

2.1. Карта (на материальном носителе или без материального носителя) может быть использована для совершения операций через банкоматы/терминалы Банка (в т.ч. с использованием Локальной карты/QR-кода), а также через банкоматы/терминалы партнеров Банка, установленные в безопасных местах и оборудованные системой видеонаблюдения и охраны (например, в офисах Банка, государственных учреждениях, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2.2. Проведение операций через банкомат/терминал осуществляются согласно инструкциям, последовательно появляющимся на экране банкомата / терминала.

2.3. Использование карты в банкоматах/терминалах считается случаем повышенного риска, если:
- вблизи банкомата/терминала находятся посторонние лица;
- на банкомате/терминале установлены дополнительные устройства, не соответствующие конструкции банкомата/терминала и расположенные на клавиатуре, сканере и/или картоприёмнике, или у клиента возникают в этом подозрения (напр., неровно установлена клавиатура для ввода ПИН и т.п.);
- для приема данных Локальной карты/QR-кода сканером, ввода данных на клавиатуре/экране требуется применение физической силы;
- есть вероятность, что люди, находящиеся в непосредственной близости, могут увидеть данные при их вводе на клавиатуре банкомата/терминала;
- банкомат/терминал работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается).

2.4. Запрещается использование карты в банкоматах/терминалах, расположенных в помещениях, для доступа (входа) в которые, требуется введение/указание реквизитов карты, ПИН, иных конфиденциальных данных. Пользуйтесь картой исключительно в банкоматах/терминалах, находящихся в безопасных местах: государственных учреждениях, банках, и других местах, находящихся под постоянным видеонаблюдением / под охраной.

2.5. Ни в коем случае не используйте ПИН вашей карты для доступа в любые помещения, даже если в этих помещениях находится нужный вам банкомат/терминал.

2.6. Если поблизости от банкомата/терминала находятся посторонние лица, выберите для снятия денег (или для совершения иной операции) более подходящее время или воспользуйтесь другим банкоматом/терминалом.

2.7. Осмотрите банкомат/терминал на наличие подозрительных устройств (например, неровно наклеенная клавиатура для ввода ПИН). При малейшем подозрении воздержитесь от снятия денег (или от совершения иной операции) и сообщите о своих подозрениях по указанному на банкомате/терминале телефону.

2.8. Не применяйте физическую силу, чтобы вставить карту в банкомат/терминал.

2.9. Если карта не вставляется в картоприемник, не используйте такое устройство. Исключение составляют случаи использования бесконтактной технологии (PayPass), когда вставлять карту в картоприемник не требуется.

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

2.11. Если банкомат/терминал работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), отмените текущую операцию, нажав на клавиатуре кнопку "Отмена", дождитесь возврата карты (если ранее карта была вставлена в картоприемник) и откажитесь от использования такого банкомата/терминала.

2.12. Получив деньги (при совершении операции по снятию наличных денежных средств), пересчитайте банкноты полистно, убедитесь, что карта

возвращена банкоматом (если ранее карта была вставлена в картоприемник), дождитесь выдачи квитанции/чека (если вы ее/его запрашивали), положите деньги в сумку (кошелек, карман) и только после этого отходите от банкомата/терминала. Сохраняйте квитанции/чеки для последующей сверки указанных в них сумм с выпиской по вашей карте.

2.13. Не слушайте советы третьих лиц и не принимайте их помощь при проведении операций с вашей картой в банкоматах/терминалах.

2.14. Если банкомат/терминал не вернул вашу карту, позвоните по указанному на банкомате/терминале номеру телефона и сообщите о случившемся. Позвоните в Банк по имеющемуся у вас номеру телефону и также сообщите о случившемся. Далее следуйте инструкциям сотрудника Банка.

3. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ КАРТЫ В ОРГАНИЗАЦИЯХ ТОРГОВЛИ И УСЛУГ

3.1. Оплата товаров/услуг в торгово-сервисных предприятиях (далее – ТСП) осуществляется непосредственно с использованием карты на материальном носителе либо посредством использования технологии токенизации реквизитов карты как на материальном носителе, так и без материального носителя.

3.2. Для снижения рисков при оплате товаров/услуг в ТСП Банк рекомендует:

3.2.1. Не используйте карту в ТСП, не вызывающих доверия.

3.2.2. Требуйте проведения операций с вашей картой только в вашем присутствии.

3.2.3. Если при использовании карты потребовался ввод ПИН убедитесь, что находящиеся в непосредственной близости люди не смогут его увидеть.

3.2.4. Перед тем как подписать чек (при необходимости), в обязательном порядке проверьте указанную в чеке сумму и иную информацию.

3.2.5. Если при попытке оплаты в проведении операции было отказано (по любой причине), сохраните ваш экземпляр чека для последующей проверки отсутствия этой операции в выписке по вашей карте.

4. РЕКОМЕНДАЦИИ ПО СОВЕРШЕНИЮ ОПЕРАЦИЙ С КАРТОЙ В СЕТИ ИНТЕРНЕТ

4.1. Для оплаты товаров/услуг в ТСП в Интернете заведите выделенную карту. Кладите на неё необходимую, небольшую сумму в преддверии операции.

4.2. Не используйте для оплаты товаров / услуг в Интернете зарплатную карту.

4.3. Операции по оплате товаров/услуг с использованием карты в ТСП через сеть Интернет осуществляются путем ввода сведений держателя карты и реквизитов карты в соответствующие поля электронной формы на сайте ТСП. Данные вводятся в требуемом формате. В качестве адреса для расчетов указывается адрес регистрации держателя карты.

4.4. Операции по оплате товаров/услуг с использованием карты через сеть Интернет являются операциями повышенного риска в случаях, если:

- сайт ТСП или сайт ввода реквизитов карты не поддерживает технологии повышенной защиты карт от мошенников MasterCard®SecureCode / Verified by Visa / MirAcept. Основу данной защиты составляет технология 3D Secure;
- сайт ТСП или сайт ввода реквизитов карты не обеспечивает защиты информации о карте при ее передаче по сети Интернет. Безопасные сайты отмечены значком в виде закрытого замка;
- для совершения операции используется компьютер/мобильное устройство с общим доступом или чужой компьютер/мобильное устройство.

4.5. С целью снижения повышенного риска при использовании карты для оплаты товаров/услуг через сеть Интернет Банк рекомендует:

4.5.1. Пользуйтесь интернет-сайтами только известных и проверенных организаций торговли и услуг.

4.5.2. Убедитесь в правильности адреса интернет-сайта ТСП, в котором планируется совершение покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

4.5.3. Не храните на карте значительную сумму денежных средств. Рекомендуется размещать на карте необходимую для покупки сумму непосредственно перед совершением операции.

4.5.4. Совершайте покупки только со своего компьютера (и) или мобильного устройства. Старайтесь не производить оплату товаров/услуг в сети Интернет при работе на компьютерах / мобильных устройствах, безопасность которых вызывает сомнения (интернет-кафе, чужой компьютер / мобильное устройство). Если покупка все же совершается с использованием чужого устройства, после завершения операции убедитесь, что ваши персональные данные и другая информация стерты с чужого устройства.

4.5.5. Пользуйтесь услугой СМС-информирования об операциях по карте.

4.5.6. Установите сложный пароль для входа в учетную запись на личном компьютере и мобильном устройстве. Пароль должен содержать не менее 7 символов минимум из 2 следующих символьных групп: цифры, заглавные и строчные буквы латинского алфавита.

4.5.7. Установите на свой компьютер и мобильное устройство лицензионное антивирусное программное обеспечение, регулярно производите его обновление и полную антивирусную проверку компьютера и мобильного устройства, а также обновление операционной системы и используемых программ (браузера и иных прикладных программ).

4.5.8. Никогда не используйте ПИН при заказе товаров/ услуг через сеть Интернет, а также по телефону/факсу.

4.5.9. Не сообщайте в сети Интернет следующие данные: пароли доступа к ресурсам Банка, в том числе одноразовые, кредитные лимиты, историю операций по вашей карте, ваши персональные данные.

4.5.10. Не устанавливайте полученные от неизвестных источников приложения на ваш компьютер и на мобильное устройство, на которое Банк отправляет вам сообщения с подтверждающими одноразовыми паролями.

4.5.11. Не используйте приложение Банка и (или) Интернет-банк для совершения операций с картой на устройствах с административными правами (например, «root» для устройств с операционной системой Android или «JailBreak» для устройств с операционной системой IOS).

4.5.12. Внимательно проверяйте полученные от Банка сообщения с одноразовыми паролями. Вводите одноразовые пароли только в том случае, если все реквизиты из сообщения полностью соответствуют совершаемому вами платежу.

4.5.13. Перед подтверждением операции по оплате товара/услуг в обязательном порядке проверяйте всю информацию, указанную в электронной форме. Если в электронной форме на сайте ТСП не проставлены (или не соответствуют действительности) сумма, валюта, дата операции, тип операции, название ТСП, подтверждение такой операции не допускается.

4.5.14. В случае, если после оплаты товара/услуг информация по подтвержденной операции, указанная в документе, подтверждающем совершение операции (например, чеке, квитанции и т.п.), не соответствует действительности, незамедлительно инициируйте отмену указанной операции.

4.6. Запрещается использовать карту для оплаты товаров/услуг в ТСП на компьютере / мобильном устройстве, если имеется подозрение, что компьютер / мобильное устройство заражено вирусной программой. Симптомы заражения:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- произвольно, без участия пользователя, запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в Интернет, хотя пользователь этого не инициировал;
- частые зависания и сбои в работе, медленная работа при запуске программ;
- невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого.

4.7. При совершении операций с использованием карты посредством каналов системы дистанционного банковского обслуживания Почта Банк Онлайн и Приложения «Почта Банк. Младший» в обязательном порядке соблюдайте действующие в Банке «Рекомендации по безопасному использованию Почта Банк Онлайн и Приложения «Почта Банк. Младший».

4.8. При использовании Интернет-банка для совершения операций с картой - всегда проверяйте наименование ресурса во избежание попадания на ложный (поддельный) ресурс.

4.9. В случае установки мобильного приложения Банка для оплаты товаров и услуг на ваше мобильное устройство – всегда проверяйте наименование авторских прав во избежание кражи учетных данных.

4.10. При возникновении подозрений в компрометации, а также в случае утери / кражи карты (информации о реквизитах карты) и/или возникновения риска их несанкционированного использования необходимо незамедлительно уведомить об этом Банк и осуществить блокировку карты.

5. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ ВИРТУАЛЬНЫХ КАРТ

5.1. Под виртуальной картой понимается любая банковская карта, выпущенная Банком Клиенту без материального носителя по программе «Кредитная карта», «Дебетовая карта» и/или «Предоплаченная карта», а также банковская карта, выпущенная Банком Клиенту / Ребенку без материального носителя в рамках продукта «Детская карта».

5.2. Случаем повышенного риска использования виртуальной карты является риск несанкционированного доступа и использования карты третьими лицами при компрометации, а также при утере/краже/изъятии устройства, с которого осуществлялся доступ к дистанционным каналам обслуживания (к системе дистанционного банковского обслуживания Почта Банк Онлайн, к Странице Банка в ЛК ГИС ЖКХ, к Приложению «Почта Банк. Младший»).

5.3. Для снижения рисков при использовании виртуальной карты необходимо в обязательном порядке соблюдать все рекомендации, указанные в настоящей памятке.

По всем вопросам, связанным с использованием банковских карт, необходимо обращаться в Клиентскую службу Банка по одному из следующих телефонов:

8 800 550 0770 (для бесплатных звонков с любого телефона на территории РФ);
+7 495 532 13 00 (для звонков из-за границы).