ПАМЯТКА
ДЕРЖАТЕЛЯ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ И ХРАНЕНИЮ КОРПОРАТИВНОЙ КАРТЫ
ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»
(действует с 31.10.2024)

Настоящая Памятка является неотъемлемой частью Правил открытия и обслуживания банковского счета юридического лица / индивидуального предпринимателя / физического лица, занимающегося в установленном порядке частной практикой, являющихся неотъемлемой частью Договора комплексного банковского обслуживания юридического лица / индивидуального предпринимателя / физического лица, занимающегося в установленном порядке частной практикой (далее – Договор КБО), а также Правил обслуживания и использования банковских карт, выпущенных ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» для юридических лиц и индивидуальных предпринимателей – резидентов и нерезидентов Российской Федерации, не имеющих заключенного с Банком договора комплексного банковского обслуживания указанной категории клиентов.

Соблюдение рекомендаций, содержащихся настоящей в Памятке, позволит обеспечить максимальную сохранность Карты, ее реквизитов, ПИН-кода и других данных, а также снизит возможные риски при совершении операций с использованием Карты / реквизитов Карты (далее – Операции) в ПТС, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Рекомендации, содержащиеся в настоящей Памятке, распространяются в том числе на Карты «Таможенная карта», в случае если указанное в ней не противоречит установленному Договором КБО порядку использования указанных Карт.

Термины и определения

Вредоносное ПО (malware) – это назойливые или опасные программы, предназначенные для доступа к устройству без ведома его владельца. Целями такого доступа могут быть удаленное управление устройством, кража данных Держателя или подмена составляемых пользователем платежных поручений;

Социальная инженерия – это метод манипуляции действиями человека, заключающийся в использовании слабостей человеческого фактора в целях незаконного получения личной информации (учетных или банковских данных) или несанкционированного доступа к компьютеру жертвы с целью установки на него Вредоносного ПО. Мошенники часто прибегают к подобной практике в связи с тем, что таким образом значительно проще добыть учетные данные, чем получить их путем взлома системы безопасности;

Фишинг – один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт. В основном используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

Термины и определения, используемые в настоящей Памятке, значения которых не указаны, имеют те же значения, что и соответствующие термины и определения, содержащиеся в Договоре КБО / Правилах обслуживания и использования банковских карт, выпущенных ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» для юридических лиц и индивидуальных предпринимателей – резидентов и нерезидентов Российской Федерации, не имеющих заключенного с Банком договора комплексного банковского обслуживания указанной категории клиентов.

Общие рекомендации

Все Карты Банка защищены от несанкционированного использования.

На Карту нанесен уникальный номер и личная подпись Держателя (при наличии соответствующего поля на Карте). Принимая Карту к оплате в торговой точке или выдавая наличные средства в Банке, кассир сверяет подпись Держателя на платежном документе с образцом подписи на Карте (при наличии).

При получении наличных средств через ПТС проверяется ПИН-код, который известен

только Держателю. ПИН-код является строго секретным. Следует хранить ПИН-код в тайне, исключив его запись на Карте или каком-либо другом документе, хранящемся вместе с Картой. Никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим в использовании Карты. При наборе ПИН-кода всегда прикрывайте клавиатуру рукой или любым предметом.

Не допускайте передачу Карты третьим лицам и неправомерное использование третьими лицами Карты, ее реквизитов или ПИН-кода. Храните в тайне от третьих лиц кодовое слово, Карту, ее реквизиты, ПИН-код и 3D-Secure / MirAccept пароль.

Несоблюдение этих правил освобождает Банк от ответственности за потери, которые могут возникнуть вследствие несанкционированного использования Карты.

Будьте внимательны к условиям хранения и использования Карты. Необходимо обеспечить надлежащее хранение Карты и не допускать механического воздействия на Карту, не повреждать магнитную полосу, не хранить Карту вместе с металлическими предметами, не допускать нахождения Карты вблизи источников открытого огня, не подвергать Карту длительному воздействию прямых солнечных лучей, не хранить Карту рядом с приборами, излучение и/или магнитные поля которых могут исказить информацию, хранимую в микропроцессоре Карты.

Не рекомендуется отвечать на электронные письма, в которых от имени Банка предлагается предоставить персональные данные. Не следуйте по ссылкам, указанным в письмах (включая ссылки на сайт кредитной организации), так как они могут вести на сайты-двойники.

Рекомендации при совершении операций с Картой в ПТС

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

Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен ПТС.

Перед использованием ПТС осмотрите его и при наличии дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН), воздержитесь от использования такого ПТС.

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

Не применяйте физическую силу, чтобы вставить Карту в ПТС. Если Карта не вставляется, воздержитесь от использования такого ПТС.

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

В случае если ПТС работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого ПТС, отменить текущую Операцию, нажав на клавиатуре кнопку «Отмена», и дождаться возврата Карты.

Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении Операций с Картой в ПТС.

Получение наличных денежных средств в ПТС и кассах банков

Подойдя к ПТС, сверьте эмблему платежной системы на Карте со стикером на ПТС и, удостоверившись, что ПТС обслуживает карты данной платежной системы, вставьте Карту в ПТС магнитной полосой вниз таким образом, чтобы полоса располагалась справа. Дождитесь появления соответствующего приглашения на экране ПТС и наберите на клавиатуре ПИН-код Карты. Следуйте дальнейшим инструкциям, высвечивающимся на мониторе ПТС. После завершения Операции возьмите Карту, деньги и квитанцию. Если вы не забрали свою Карту в

течение 30 секунд, в целях безопасности она будет сохранена в ПТС. Если вы просрочили время и не взяли деньги в течение 30 секунд, то они будут возвращены в ПТС. Не отходите от ПТС, пока Операция полностью не завершится.

Если ПТС не выдал наличные денежные средства (при условии наличия запрошенной суммы на Картсчете и обслуживания ПТС карт данной платежной системы) или изъял Карту, то следует обратиться в Банк по телефонам Контакт-центра Банка, указанным на сайте Банка или на обороте Карты, и сообщить город, улицу и номер дома, где находится ПТС; банк, которому принадлежит ПТС, а также номер Карты, время проведения и сумму Операции. Специалисты Банка постараются оказать необходимую помощь. При всех телефонных разговорах с сотрудниками Банка для установления личности Держателя следует называть кодовое слово, которое было указано в заявлении на выпуск и обслуживание Карты. Для облегчения и оперативности взаимодействия с Банком желательно записать номер Карты и телефон Банка в свою записную книжку.

Наличные денежные средства возможно получить в кассе Банка, а также в кассах или ПТС других банков, принимающих к обслуживанию карты данной платежной системы. Это можно определить, найдя стикер с эмблемой платежной системы на ПТС, дверях банка или на стекле кассы. При получении денег в кассе другого банка после предъявления кассиру Карты необходимо сообщить сумму, которую вы хотите получить. Кассир осуществляет необходимые процедуры и предлагает подписать распечатку электронного терминала (чек), удостоверившись в соответствии суммы, проставленной на документе, сумме Операции. Нужно иметь в виду, что сумма на чеке будет складываться из суммы Операции и суммы комиссии банка – владельца данного устройства. В качестве подтверждения успешного проведения Операции выдается чек терминала с подписью Держателя.

Держатель обязан сохранять документы по Операциям (чеки и др.) до завершения всех расчетов по Карте и предоставлять их по требованию Банка в целях урегулирования спорных вопросов.

Банк предупреждает, что в случае проведения Операций по получению наличных денежных средств в ПТС и кассах с Картсчета может удерживаться комиссия в соответствии с тарифами Банка.

При проведении Операций в кассах банков или предприятиях торговли и сервиса кассир может потребовать документ, удостоверяющий личность Держателя.

Оплата товаров и услуг

Удостоверьтесь, что выбранное предприятие торговли или сервиса обслуживает карты данной платежной системы. Для этого найдите на двери торговой точки или на стекле кассы стикер с эмблемой платежной системы Карты. Не используйте Карты в организациях торговли и услуг, не вызывающих доверия. Для осуществления Операции необходимо передать Карту кассиру (неприменимо для Карт, снабженных технологией бесконтактных платежей, и Платежных колец). Требуйте проведения Операций с Картой только при личном присутствии. Это необходимо в целях снижения риска неправомерного получения персональных данных, указанных на Карте.

При использовании Карты для оплаты товаров и услуг кассир может потребовать от Держателя предоставить паспорт, подписать чек или ввести ПИН-код. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. После осуществления кассиром необходимых процедур необходимо подписать распечатку электронного терминала (чек), удостоверившись в соответствии суммы, проставленной на документе, сумме Операции. Не подписывайте чек, в котором не проставлена сумма Операции. Сохраняйте документы по Операциям (чеки и др.) до завершения всех расчетов по Карте.

В случае если при попытке оплаты Картой имела место «неуспешная» Операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки отсутствия указанной Операции в выписке по Картсчету.

Совершение операций с Картой через сеть Интернет

Использование Карт для оплаты товаров и услуг через Интернет неизбежно сопряжено с рисками получения несанкционированного доступа злоумышленников к устройствам пользователей, заражения устройств Вредоносным ПО, использования методов Социальной инженерии, Фишинга и реализации прочих угроз, способных привести к финансовым потерям Клиентов.

Для снижения риска несанкционированного доступа к карточным данным и мошеннических действий посторонних лиц необходимо обязательно принимать следующие меры предосторожности.

На устройстве, которое используется для осуществления платежей через Интернет, следует:

1) Применять только лицензионное программное обеспечение, в том числе средства антивирусной защиты (если применимо), обеспечивая при этом регулярное обновление антивирусных баз, а также еженедельную полную антивирусную проверку.

При подозрении на наличие вирусов, в частности, при неожиданном прекращении реагирования программ или всей операционной системы на действия пользователя («зависание» устройства), ощутимом снижении скорости работы, самопроизвольных перезагрузках, подозрительной сетевой активности, появлении необычных процессов или приложений, иных сбоях, необходимо воздержаться от использования устройства для оплаты через Интернет и принять меры по проверке на наличие вирусов и их удалению при обнаружении.

Обнаружение Вредоносного ПО на устройстве, используемом для совершения платежей через Интернет, относится к событиям компрометации. В этом случае необходимо незамедлительно обратиться в Банк в порядке, предусмотренном соответствующими правилами.

Если это возможно, установить межсетевой экран с разрешением соединений с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений ПО, а также ограничить доступ к устройству, предназначенному для совершения платежей через Интернет.

2) Обеспечивать своевременную (по возможности автоматическую) загрузку и установку всех последних обновлений операционных систем, а также регулярное обновление другого системного и прикладного программного обеспечения, используемого на устройстве, по мере появления новых версий.

3) Исключать возможность посещения сайтов сети Интернет сомнительного содержания, загрузку и установку нелицензионного ПО.

4) Если на устройстве, используемом для совершения платежей через Интернет, также используется электронная почта либо иные средства коммуникаций (например, мессенджеры), не открывать вложения и не использовать ссылки, указанные в подозрительных письмах, полученных по электронной почте, всегда вводить адрес через браузер. Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные web-сайты, имеющие похожие адреса, например, mcb.ru вместо истинного mkb.ru.

5) По возможности осуществлять антивирусную проверку любых файлов и программ, загружаемых на устройство, используемое для совершения платежей через Интернет.

6) Не допускать работу в операционной системе под учетной записью, имеющей права администратора, следует использовать учетную запись с ограниченными правами.

7) Не допускать отсутствие пароля на вход в операционную систему / использование простых паролей для всех учетных записей, имеющих право входа в операционную систему. Регулярно осуществлять смену паролей.

8) Не использовать средства удаленного (дистанционного) доступа. Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного). Администрирование устройства, используемого для совершения платежей через Интернет, следует осуществлять локально с использованием физического доступа администратора к устройству.

9) Осуществлять проверку корректности посещаемых (указанных) в браузере адресов до введения реквизитов Карты.

Не допускайте возможность доступа к устройству, используемому для совершения платежей через Интернет, третьих лиц.

Необходимо обеспечить контроль конфигурации устройств, с использованием которых осуществляются платежи через Интернет. В этих целях рекомендуется использовать специализированное программное обеспечение для контроля целостности системных и прикладных файлов (например, свободно распространяемое программное обеспечение OSSec) или, если речь идет о мобильных устройствах, осуществлять такой контроль через настройки и перечни установленных программ и предоставленных им разрешений.

Незамедлительно обращайтесь в Банк при возникновении любой нестандартной ситуации при осуществлении платежей через Интернет.

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

Не сообщайте персональные данные или информацию о Карте через сеть Интернет, например, ПИН-код, пароли доступа к ресурсам Банка, срок действия Карты, лимиты, историю Операций, персональные данные.

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

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

Блокировка / разблокировка Карты в случае утраты

В случае обнаружения факта утраты, компрометации Карты необходимо незамедлительно поставить об этом в известность Банк, обратившись по телефонам Контакт-центра Банка, указанным на сайте Банка или на обороте Карты.

Разблокировка Карты, заблокированной по причине утраты, осуществляется Банком только по письменному заявлению Клиента, оформленному в любом офисе Банка.