Рекомендации по безопасному использованию Платежных карт АО «КОШЕЛЕВ-БАНК»

Телефоны клиентской поддержки по операциям с Платежными картами АО «КОШЕЛЕВ-БАНК»:

- **7 (495) 232-37-23** круглосуточно Горячая линия круглосуточной поддержки клиентов – держателей платежных карт Банка;
- **Контакт-центр Банка, круглосуточно**
  - **7 (846) 251-00-00** г.Самара;
  - **7 (4842) 22-03-03** г. Калуга;
  - **7 (8482) 55-80-90** г. Тольятти;
  - **7 (84635) 57-058** г. Новокуйбышевск;
  - **7 (8422) 27-64-64** г.Ульяновск
  - **7(495) 870-57-44** г. Москва.

Для карт Black Edition дополнительно
Круглосуточные телефоны MasterCard для обращения в Консьерж-службу и в страховую компанию AXA Assistance:

- **8 800 200 35 57 и +7 499 270 35 00** автоответчик MasterCard круглосуточно (для звонков по страховым случаям) и для обращения в Консьерж-службу, при звонке на линию Вас попросят ввести первые 6 цифр номера карты, при верном вводе звонок переводится на страховщика (AXA Assistance).
- koshelevBNK@concierge-mc.com - выделенный E-mail, для обращений держателей карт в Консьерж-службу.

Настоящие Рекомендации по безопасному использованию Платежных карт АО «КОШЕЛЕВ-БАНК» (далее – Рекомендации) разработаны Банком на основании письма Банка России от 02.10.2009г. №120-т в рамках работы по информированию о рисках, связанных с использованием Платежных карт, и направленную на повышение осведомленности Держателей карт о мерах по сохранности банковской карты, ее реквизитов, персонального идентификационного номера (далее – ПИН-код) и других данных.

Соблюдение Рекомендаций позволит существенно снизить риски при совершении операций с использованием Платежной карты в устройствах самообслуживания (банкоматы, ИПТ), при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

Настоящие Рекомендации являются неотъемлемой частью Договора на выпуск и обслуживание карты АО «КОШЕЛЕВ-БАНК» (далее - Договор) и размещаются на официальном сайте Банка www.koshelev-bank.ru в доступной для ознакомления форме.

Общие рекомендации

1. Храните свою Платежную карту в недоступном для окружающих месте. Не передавайте Платежную карту другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, особенно в поездках.

Во избежание мошенничества с использованием Вашей Платежной карты требуйте проведения операций с Платежной картой только в Вашем присутствии, не позволяйте уносить ее из поля Вашего зрения.

2. Никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, работникам Банка, кассирам.

3. ПИН-код 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, не пишите ПИН-код на Платежной карте, не вводите ПИН-код при работе в сети Интернет.

4. При получении Платежной карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя Платежной карты. Это снизит риск использования 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 не следует хранить рядом с мобильным телефоном, бытовой и офисной техникой.

6. В случае компрометации, утери Карты или получении SMS-сообщение от Банка по операции, которую Вы не совершали, необходимо срочно заблокировать карту, позвонив по телефону:

- **7 (495) 232-37-23** круглосуточно Горячая линия круглосуточной поддержки клиентов – держателей платежных карт Банка;
- **Контакт-центр Банка, круглосуточно**
  - **7 (846) 251-00-00** г.Самара;
  - **7 (4842) 22-03-03** г. Калуга;
  - **7 (8482) 55-80-90** г. Тольятти;

- **7 (84635) 57-058** г. Новокуйбышевск;
- **7 (8422) 27-64-64** г.Ульяновск.
- **7(495) 870-57-44** г. Москва.

и следовать полученным инструкциям.

Ваше устное обращение о блокировке Платежной карты должно содержать информацию: ФИО Держателя карты, тип Карты, либо номер Карты, паспортные данные, кодовое слово.

До момента обращения в Банк Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Помните, что блокировка Карты не исключает, но минимизирует Ваши возможные потери от несанкционированного Вами использования Вашей Карты другими лицами.

Указанные телефоны и номер Платежной карты необходимо всегда иметь при себе (на случай утере/кражи/изъятия) на других носителях информации: в записной книжке, мобильном телефоне и т.д., но не рядом с записью о ПИН-коде.

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 работника Банка, сообщить персональные данные или информацию о Платежной карте (в том числе ПИН-код) не сообщайте их. Перезвоните в Банк и сообщите о данном факте.

Ни при каких обстоятельствах не сообщайте персональные данные никому, включая работников Банка.

9. Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по SMS/электронной почте, в том числе от имени Банка.

Мошеннические сообщения, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS-сообщении номер телефона/перейти по указанной ссылке для уточнения информации.

В случае получения подобных сообщений настоятельно рекомендуем Вам:

- не перезванивать на номер телефона, указанный в SMS-сообщении;
- не следуйте по ссылкам, указанным в письмах (включая ссылки на сайт Банка), т.к. они могут вести на сайты-двойники;
- не предоставлять информацию о реквизитах Платежной карты (номере Платежной карты, сроке ее действия, ПИН-коде, CVV2/CVC2 коде, контрольной информации по Платежной карте), или об одноразовых паролях, в т.ч. посредством направления ответных SMS-сообщений;
- не проводить через банкоматы и иные устройства самообслуживания никакие операции по инструкциям, полученным по телефону.

Если полученное сообщение вызывает любые сомнения или опасения, необходимо обратиться в Банк по телефонам, указанным на обратной стороне Платежной карты, и следовать указаниям специалиста.

10. В целях информационного взаимодействия с Банком рекомендуется использовать только контактные данные (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке, или указанные на официальном сайте Банка www.koshelev-bank.ru.

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

12. В случае если имеются предположения о раскрытии ПИН-кода, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, либо в случае утраты Платежной карты, необходимо немедленно провести блокировку банковской карты в соответствии с п.5.12 Порядка или п.6 настоящих Рекомендаций.

13. Не реже 1 (Одного) раза в месяц проверяйте движение денежных средств, находящихся на Вашем Счете карты, путем получения выписки непосредственно в Банке, либо не реже 1 (Одного) раза в день – с использованием средств дистанционного банковского обслуживания.

14. Если Вы допустили несанкционированный овердрафт (неразрешенный отрицательный остаток на Счете карты), то на сумму овердрафта начисляются штрафные проценты в соответствии с Тарифами, утвержденными к Порядку выпуска и обслуживания Платежных карт международной платежной системы MasterCard Worldwide Акционерного общества «КОШЕЛЕВ-БАНК». При погашении овердрафта наличным или безналичным способом или при перечислении средств со страхового депозита сначала производится погашение начисленных штрафных процентов, а затем основной суммы овердрафта.

15. При прекращении действия Платежной карты в связи с истечением или досрочным окончанием ее срока действия остаток денежных средств на Счете карты Вам будет выдан Банком после проведения окончательных взаиморасчетов.

Рекомендации при совершении операций с Платежной картой с устройствами самообслуживания (УС)

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.Осуществляйте операции в банкоматах и ИПТ, имеющих наклейки с логотипами, идентичными логотипу на Вашей Платежной карте.

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

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

5.Перед использованием УС осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции, цвету и расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема Карт (например, наличие неровно установленной клавиатуры набора ПИН-кода). Воздержитесь от использования такого банкомата. Сообщите о своих подозрениях работникам Банка по телефону, указанному в настоящих Рекомендациях или на банкомате.

6.Не применяйте физическую силу, чтобы вставить Платежную карту в УС. Если Платежная карта не вставляется, воздержитесь от использования такого УС.

При приеме и возврате Платежной карты устройством не пытайтесь ускорить прерывистое движение карты в картоприемнике. Неравномерное движение Платежной карты является не сбоем, а необходимым средством защиты Вашей Платежной карты от компрометации.

7.**При проведении операции с вводом ПИН-кода ВСЕГДА прикрывайте клавиатуру, например, свободной рукой.** Это не позволит мошенникам увидеть Ваш ПИН-код или записать его на видеокамеру.

8.Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. При необходимости обратитесь к работникам Банка или позвоните по телефонам, указанным на устройстве самообслуживания или на оборотной стороне Вашей Платежной карты.

9.Помните, что в случае трехкратного ввода неправильного ПИН-кода, Ваша Платежная карта блокируется, в некоторых случаях может быть изъята банкоматом. Если банкомат не возвратил Платежную карту, необходимо позвонить в Банк по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, либо обратиться в офис Банка для ее блокировки и далее следовать инструкциям его работника.

10. 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.

11. 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.

12. Следует сохранять распечатанные банкоматом квитанции в течение 6 месяцев (в т.ч. и чек об изъятии Карты) для последующей сверки указанных в них сумм с выпиской по банковскому счету.

13. **Внимание! Не совершайте на УС никаких операций по указаниям посторонних лиц, позвонивших Вам и представившихся работниками Банка или других организаций. Помните! Вводя ПИН-код, Вы даёте Банку право и указание провести операцию, информация о которой отражена на экране УС.**

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 Вас 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. По завершении операции кассир должен выдать Вам торговый чек или торговый слип. Не подписывайте чек (слип), в котором не проставлены (или не соответствуют действительности) сумма, валюта, дата операции, тип операции, название торгово-сервисного предприятия.
4. При отказе в обслуживании по банковской карте в торгово-сервисных точках (на территории РФ), не связанном с техническими проблемами (когда Вас сразу информируют, что оплата по Карте не может быть проведена из-за неисправности оборудования, отсутствия связи), рекомендуем Вам информировать службу поддержки клиентов АО «Кошелев-банк» по номерам телефонов, указанным выше по каждому такому случаю (желательно не покидая торгово-сервисную точку). Сообщите следующую информацию: номер Вашей карты, название торговой точки, название банка, через который она работает по обслуживанию банковских карт.
5. По возможности получите чек с отказом в проведении операции и передать в Банк. К случаям, о которых следует информировать службу поддержки клиентов, относятся и ситуации, когда операция по Карте одной платежной системы была отклонена, но при этом успешно прошла по карте другой платежной системы.
6. При возврате покупки или отказе от услуг, ранее оплаченных в торгово-сервисном предприятии по Вашей Карте, должна быть проведена операция «возврат покупки» с обязательным оформлением чека (слипа), подписанного кассиром торгово-сервисного предприятия. Обязательно сохраните чек (слип) о возврате покупки. Если сумма операции не поступит на счет Вашей Карты в течение 30 (Тридцати) дней, обратитесь в Банк для оформления письменного обращения о спорной операции.
7. Сохраняйте все чеки (слипы) в течение 6 (Шести) месяцев. Не выбрасывайте слипы и чеки, на которых отображен полный номер Карты.

В случае любого неправомерного с Вашей точки зрения отказа в проведении операции по Платежной карте рекомендуем Вам незамедлительно связываться с Банка.

Рекомендации при совершении операций с Платежной картой через сеть Интернет

1. **Внимание! Для проведения операции в сети Интернет не требуется вводить ПИН-код Платежной карты!**

Для проведения операции в сети Интернет, как правило, требуются данные: номер карты, срок действия, имя и фамилия Держателя, указанные на карте, код безопасности – CVV/CVC –последние три цифры, указанные на полосе для подписи на оборотной стороне карты. Дополнительно могут быть запрошены название банка, выпустившего карту, и адрес, указанный Вами в Заявлении на получение карты. **Для зачисления денежных средств на Вашу карту достаточно только НОМЕРА карты. Коды CVV/CVC и смс код для подтверждения операции зачисления не требуются.**

2. В целях обеспечения безопасного проведения операций с использованием реквизитов карты в сети Интернет рекомендуем пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг, сайтами торгово-сервисных предприятий, использующих технологию безопасного проведения операций по картам: «**Verified by Visa**» и «**MasterCard SecureCode**».

При совершении платежа в интернет-магазине, поддерживающем технологию Verified by Visa и/или MasterCard SecureCode, после ввода информации о Платежной карте Вы будете перенаправлены на аутентификационный сервер Банка для подтверждения правомерности операции. В течение нескольких секунд на номер мобильного телефона, указанный Вами в заявлении, будет выслан пароль для платежа.

Внимание! Срок действия пароля, полученного по SMS, ограничен.

При успешной аутентификации Вы будете переадресованы на сайт интернет-магазина для получения информации о результатах платежа. В противном случае (неправильный ввод пароля, отказ от прохождения аутентификации) проведение операции по Платежной карте не осуществляется.

3. Операции в сети Интернет в защищенном режиме проводятся с использованием одноразовых паролей, которые можно получить в виде SMS-сообщения на Ваш мобильный телефон, указанный в Заявлении на открытие Платежной карты.

4. Не сообщайте персональные данные или информацию о Платежной карте (Счете) через сеть Интернет, например ПИН-код, пароли доступа к ресурсам Банка, срок действия Платежной карты, кредитные лимиты, историю операций, персональные данные.

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 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.

Схемы мошенничества

По данным APACS (Association for Payment Clearing Services – Ассоциация систем клиринговых платежей, Великобритания) наиболее распространенными схемами мошенничества с банковскими картами являются следующие:

Компрометация ПИН-кода Держателем карты. Имеется ввиду, к примеру, запись ПИН-кода на Платежной карте или каком-либо носителе (лист бумаги, записная книжка, мобильный телефон), хранимом вместе с Платежной картой. Соответственно, если Платежная карта утеряна или украдена (вместе с сумкой, бумажником), у мошенника оказывается и Платежная карта и ПИН-код. В таком случае мошенникам совсем нетрудно несанкционированно использовать Платежную карту для получения наличных денежных средств и/или оплаты товаров (услуг).

Дружественное мошенничество. Использование в своих целях Платежной карты или ее реквизитов с предварительной осведомленностью о ПИН-коде или без знания ПИН-кода соответственно членами семьи, близкими друзьями, коллегами по работе. То есть людьми, имеющими доступ к месту хранения Платежной карты.

Ложный ПИН-ПАД. Держателю Платежной карты может быть предложено ввести ПИН-код не в настоящий ПИН-ПАД (устройство для ввода ПИН-кода), а в ложное устройство, его имитирующее, которое запомнит введенный код. Такие устройства иногда устанавливают рядом со считывающими датчиками, предназначенными для прохода в помещение с устройствами самообслуживания (банкоматом, ИПТ) с использованием в качестве идентификатора (электронного ключа) Платежной карты.

Фи́шинг (англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям, реквизитам Платежной карты, ПИН-коду и т.п. Чаще всего используется в виде рассылки через Интернет электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени Банка или платежной системы, сервисов RamblerMail.ru(Rambler, Mail.ru) или внутри социальных сетей (Facebook, Вконтакте, Одноклассники.ru). В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, с просьбой подтвердить указанную конфиденциальную информацию. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить его ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, или ПИН-код для подтверждения доступа, что позволяет мошенникам получить доступ к личным кабинетам и банковским счетам или проводить несанкционированное списание денежных средств с банковского счета.

Вишинг (с англ. vishing, от voice phishing – голосовой фишинг) назван так по аналогии с фишингом. Сходство названий подчеркивает тот факт, что принципиальной разницы между вишингом и фишингом нет. Основное отличие

вишинга в том, что, так или иначе, задействуется телефон для автоматического сбора конфиденциальной информации Держателя карты.

Клиент получает от автоинформатора или живого «оператора банка» звонок, в котором сообщается, что с Платежной картой, например, производятся мошеннические действия, и даёт инструкции — перезвонить по **определённому номеру** немедленно.

Клиент звонит по указанному номеру, далее ему злоумышленник (часто представляется вымышленным именем от лица Банка), принимающий звонки по указанному автоответчиком или «оператором банка» номеру, или голос автоответчика просит сообщить или ввести в тоновом наборе/ на телефонной клавиатуре соответственно свои конфиденциальные данные (реквизиты карты или банковского счёта, пароли, ПИН- код, коды доступа и другую дополнительную информацию).

Смишинг (англ. *SMiShing* — от «SMS» и «фишинг», SMS-фишинг). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем».

Встречается и следующий вид SMS-фишинга: на подставном сайте для получения какой-либо услуги просят отправить SMS на предложенный номер или ввести свой номер сотового телефона, чаще всего это фальшивые файлообменные сервисы. В первом случае с телефонного счёта абонента списывается крупная (возможно, максимальная предусмотренная контрактом) сумма, во втором — номер добавляется в базу адресов рассылки SMS-спама и может использоваться для дальнейших фишинговых действий.

Копирование магнитной полосы (skimming, от англ. skim — снимать сливки**) –** вид мошенничества, при котором с помощью специального считывающего устройства скиммера злоумышленники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и CVC-код) с последующим копированием этих данных на другую карту-дубликат, изготовленную мошенниками.

Скиммер — миниатюрное считывающее переносное устройство, которое может крепиться к банкомату. Такие приспособления помогают мошенникам воровать данные банковских карт– всю информацию, записанную на магнитной полосе. Скиммером может быть пластиковая накладка, прикрепляемая к кардридеру, миниатюрная видеокамера в держателе для брошюр рядом с банкоматом. Также распространены специальные накладки на клавиатуру, считывающие порядок набора ПИН-кода. К банкоматам скиммеры крепятся с помощью обычного двустороннего скотча или застежки-«липучки».

Таким образом, злоумышленники изготавливают точную копию Платежной карты (точнее копию только магнитной полосы на чистом куске пластика) После копирования, карты будут иметь даже одинаковый ПИН-код. С помощью такой карты-дубликата злоумышленники могут расплачиваться в некоторых торговых центрах, где при оплате покупки не требуется вводить ПИН-код.

В 2015 году скиммеры начали устанавливать на дверях банков, с установленным считывателем карты. При помощи такого считывателя можно открыть дверь в нерабочие часы банка для получения доступа к банкомату. Вставляете Платежную карту в дверной приемник, за это время скиммер успевает считать информацию с магнитной ленты, после чего мошеннику остается только воспользоваться этими данными.

Узнать ПИН-код можно с помощью мини-камеры или накладок на клавиатуру, установленных на банкоматах.

Для защиты от скимминга банки рекомендуют использовать Платежные карты только в заслуживающих доверия торговых точках и интернет-магазинах. При оплате товаров в ресторанах, магазинах и т. д. следует не выпускать карту из вида, а деньги снимать в банкоматах, расположенных в отделениях банков, крупных торговых центрах, на охраняемой территории.

Бывают случаи использования поддельных устройств, внешне дублирующих банкомат.

Фальшивые банкоматы. Мошенники разрабатывают и производят фальшивые банкоматы, либо переделывают старые, которые выглядят как настоящие. Размещаются банкоматы в наиболее оживленных местах. После введения Платежной карты и ПИН-кода обычно на дисплее фальшивого банкомата появляется надпись, что денег в банкомате нет или, что банкомат не исправен, либо Платежная карта просто застревает в банкомате. К тому времени мошенники уже скопировали с магнитной полосы карты информацию о счете данного лица и его персональный идентификационный номер.

Скиммер способен украсть информацию только с магнитной полосы, но не с чипа. По этой причине (и не только) чиповые карты считаются более защищёнными.

Стать жертвой скимминга можно, не только снимая наличные, но и оплачивая покупки в торговых точках, услуги такси и т.п.. Для копирования данных официанты, кассиры, служащие гостиниц используют переносные скиммеры или устройства, прикрепленные к терминалу оплаты.

Держатели карт перед снятием наличных денег в банкоматах всегда должны проявлять внимательность и убедиться, что лишних устройств на банкомате нет. При их обнаружении немедленно сообщите об этом в банк и не используйте его для снятия денежных средств со счета.

Вводя ПИН-код ОБЯЗАТЕЛЬНО прикрывайте свои действия ладонью второй руки.

Обращаем Ваше внимание, что АО «КОШЕЛЕВ-БАНК» никогда:

- **НЕ запрашивает информацию по банковской карте Клиента (полный номер карты, срок ее действия, CVV, ПИН-код, количество карт, принадлежащих Клиенту, остаток денежных средств на счете Клиента, и пр.), в т.ч. в рамках исполнения Банком требований №161-ФЗ по подтверждению факта инициирования операции Клиентом;**
- НЕ отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию банковской карты, CVV, ПИН-код, контрольную информацию и пр.);
- НЕ отправляет сообщения с формой для ввода Ваших персональных данных;
- НЕ просит Вас зайти в личный кабинет системы ДБО по ссылкам в письмах.

Внимание! В случае если Вы все же пострадали от мошенничества:

1. **Необходимо немедленно обратиться в Контакт-центр Банка для блокировки Карты, реквизиты которой были сообщены посторонним или по которой были совершены несанкционированные операции, и следовать рекомендациям специалиста.**
2. **По факту мошенничества рекомендуется подать заявление в правоохранительные органы.**

Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.

Горячая линия круглосуточной поддержки Банка: (495) 232-37-23 для карт MasterCard Worldwide;

Действует для получения консультаций по обслуживанию Платежной карты и работе устройств, а также о режиме работы офисов Банка, при условии, если звонящий сообщает следующие данные о Держателе карты:

- ФИО, при этом ФИО точно должны соответствовать данным содержащимся в программе;
- Название банка, выпустившего Платежную карту;
- Номер Платежной карты или кодовое слово, или иная информация, позволяющая однозначно идентифицировать держателя Платежной карты.

Сервисы клиентской поддержки процессинга:

- блокировка действия Платежной карты в Процессинговом центре;
- информирование о доступном остатке по Платежной карте;
- информирование об Операциях, совершенных с использованием Платежной карты;
- информирование о статусе Платежной карты (активная или блокированная);
- информирование об установленных лимитах по Платежной карте, при наличии (лимит на снятие наличных денежных средств, лимит на безналичные транзакции и т.п.).