ПАМЯТКА КЛИЕНТА ДЕРЖАТЕЛЯ БАНКОВСКОЙ КАРТЫ ОБ ОСНОВНЫХ УСЛОВИЯХ ИСПОЛЬЗОВАНИЯ БАНКОВСКОЙ КАРТЫ И О ПОРЯДКЕ УРЕГУЛИРОВАНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ЕЕ ИСПОЛЬЗОВАНИЕМ, А ТАКЖЕ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ В РАМКАХ ПРИМЕНЯЕМЫХ ФОРМ БЕЗНАЛИЧНЫХ РАСЧЕТОВ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ЗАКОНОДАТЕЛЬСТВА РФ.

(Настоящая памятка для клиентов Банка разработана в соответствии с Письмом ЦБР от 22 ноября 2010 г. N 154-Т "О рекомендациях по раскрытию информации об основных условиях использования банковской карты и о порядке урегулирования конфликтных ситуаций, связанных с ее использованием", Письмом ЦБР от 2 октября 2009 г. N 120-Т "О памятке "О мерах безопасного использования банковских карт", ФЕДЕРАЛЬНОГО ЗАКОНА «О НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ», Положением Банка России от 19 июня 2012 г. N 383-П "О правилах осуществления перевода денежных средств").

«Тимер Банк» (публичное акционерное общество), (далее по тексту – Банк) настоящим доводит до сведения клиентов следующую информацию:

Государственной корпорацией Агентство по страхованию вкладов Банк включен в реестр Банков – участников системы обязательного страхования вкладов 20 января 2005г. под номером 488.

Денежные средства на банковском счете, открытом для совершения операций с использованием банковских карт, застрахованы в соответствии с Федеральным законом "О страховании вкладов физических лиц в банках Российской Федерации" (далее - Закон о страховании вкладов). В соответствии со статьей 5 Закона о страховании вкладов страхованию подлежат только денежные средства клиента, размещенные на банковских счетах, за исключением денежных средств, указанных в части 2 статьи 5 Закона о страховании вкладов. Денежные средства, внесенные для расчетов с использованием предоплаченной карты или кредитной карты без использования банковского счета клиента, не подлежат обязательному страхованию в соответствии с Законом о страховании вкладов.

ПЕРЕЧЕНЬ ПРЕДОСТАВЛЯЕМЫХ УСЛУГ.

Посредством банковской карты Вы можете воспользоваться следующим перечнем услуг, предоставляемых Банком:

- получение наличных денежных средств в валюте Российской Федерации или иностранной валюте на территории Российской Федерации;
- получение наличных денежных средств в иностранной валюте за пределами территории Российской Федерации;
- оплату товаров (работ, услуг, результатов интеллектуальной деятельности) в валюте Российской Федерации на территории Российской Федерации, а также в иностранной валюте - за пределами территории Российской Федерации;
- иные операции в валюте Российской Федерации, в отношении которых законодательством Российской Федерации не установлен запрет (ограничение) на их совершение;
- иные операции в иностранной валюте с соблюдением требований валютного законодательства Российской Федерации.

ПОРЯДОК ОЗНАКОМЛЕНИЯ С ИНФОРМАЦИЕЙ О КОМИССИЯХ И МЕСТАХ ОБСЛУЖИВАНИЯ.

Ознакомиться с комиссиями за услуги, совершаемые с использованием расчетных (дебетовых) карт, кредитных карт; о размере и сроках взимания кредитной организацией - эмитентом с держателя банковской карты платы за обслуживание банковской карты, продление, перевыпуск банковской карты; с комиссией за выдачу наличных денежных средств в банкоматах кредитной организации; с комиссией по списанию средств с карточного счета в валюте, отличной от валюты счета; за услуги мобильного банка; а также о мероприятиях, проводимых в целях повышения мотивации держателей банковских карт на совершение безналичных расчетов (программы лояльности, в случае ее принятия) Вы можете в местах обслуживания клиентов в головном офисе Банка, в дополнительных офисах и филиалах Банка, а также на официальном сайте Банка по адресу: www.timerbank.ru

Ознакомиться с информаций о местах обслуживания (приема) банковских карт (пунктах выдачи наличных денежных средств - ПВН), банкоматах кредитной организации, устройствах Банка, предназначенных для совершения операций с использованием платежных карт, Вы можете в соответствии с Приложением № 1 к настоящей Памятке.

СПОСОБЫ ПОПОЛНЕНИЯ БАНКОВСКОГО СЧЕТА.

Пополнить банковский счет, предусматривающий совершение операций с использованием расчетных (дебетовых) карт, кредитных карт Вы можете следующими способами, а именно:

- путем внесения наличных денежных средств через банкомат,

- путем внесения наличных денежных средств через кассу Банка и его филиальной сети (для физических лиц);

- путем безналичного перечисления денежных средств со счета физического лица, расчетного счета юридического лица или индивидуального предпринимателя, открытого в Банке;

- путем безналичного перечисления денежных средств со счета физического лица, расчетного счета юридического лица или индивидуального предпринимателя, открытого в другом банке.

БЛОКИРОВКА И РАЗБЛОКИРОВКА БАНКОВСКОЙ КАРТЫ.

Банк доводит до Вашего сведения, что возможна блокировка карты, происходящей:

- при наложении ареста на денежные средства должника-физического лица на основании постановления судебного пристава;

- при исполнении постановления налогового органа по счетам юридических лиц, индивидуальных предпринимателей.

Банк доводит до Вашего сведения, что возможна блокировка карты при несоблюдении условий заключенных соглашений.

Разблокировать карту Вы можете, исполнив свои долговые обязательства.

СМС-ИНФОРМИРОВАНИЕ.

Держатель банковской карты уведомляется об операциях, совершенных с использованием банковской карты, посредством услуги SMS-информирование.

Во избежание возникновения просроченной задолженности по кредиту и процентам по нему Банк оставляет за собой право информирования клиента о сроках и суммах исполнения перед кредитной организацией обязательств по уплате процентов по кредиту, предоставленному с использованием банковской карты, сроках и суммах окончательного исполнения обязательств по кредиту, сроках и суммах исполнения обязательств при наличии просроченной задолженности по кредиту.

ПРАВА ДЕРЖАТЕЛЯ БАНКОВСКОЙ КАРТЫ.

Держателю банковской карты предоставляется право установить платежный лимит по карте менее суммы доступных средств при условии предоставления в Банк заявления.

По запросу держателя банковской карты Банк вправе разъяснить ему порядок осуществления расчетов между кредитной организацией - эквайрером, платежной системой и Банком - эмитентом, приведший к списанию суммы денежных средств с банковского счета клиента, предусматривающего совершение операций с использованием расчетных (дебетовых) карт, кредитных карт, в валюте, отличной от валюты совершенной операции.

В случае утраты банковской карты Вы можете обратиться за необходимой информацией по телефону **8-800-100-66-77.**

ПОРЯДОК РАССМОТРЕНИЯ ЗАЯВЛЕНИЙ.

Банк рассматривает заявления держателя банковской карты по операциям, совершенным с использованием банковской карты в течение 30 календарных дней с даты подачи заявлений в письменном виде.

При этом если Банку требуется получение дополнительной информации от платежной системы, то срок рассмотрения заявлений клиента увеличивается, но не более чем на срок рассмотрения заявлений, предусмотренный правилами платежной системы. В случае если по заявлению держателя банковской карты Банк направил запрос в платежную систему, то Банк сообщает клиенту о продлении срока рассмотрения заявления.

При осуществлении операций с использованием карт возможны несоответствия суммы операций, совершаемых с использованием банковской карты, и суммы денежных средств, списанных с банковского счета клиента по данной операции (например, в случае если операция с использованием банковской карты совершалась в валюте, отличной от валюты банковского счета). Отражение операций по банковскому счету осуществляется на основании подтверждающих операции документов, день поступления которых в Банк может не совпадать с днем совершения клиентом операции. При этом за счет изменения курсов валют (кросс-курсов) возможно изменение размера суммы денежных средств, подлежащих списанию с банковского счета по операции, совершенной в валюте, отличной от валюты банковского счета.

ПАМЯТКА «О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ»

ОБЩИЕ РЕКОМЕНДАЦИИ.

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.

2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

3. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.

4. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.

5. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

6. Телефон Банка - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны Банка - эмитента банковской карты и номер банковской 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 банковской 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 банковской карте (в том числе ПИН) не сообщайте их. Перезвоните в кредитную организацию - эмитент банковской карты и сообщите о данном факте.

9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты) предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в письмах (включая ссылки на сайт Банка), т.к. они могут вести на сайты-двойники.

10. В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты 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 банковской карты.

11. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской 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 банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты и следовать указаниям сотрудника данной кредитной организации. До момента обращения в кредитную организацию - эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией - эмитентом банковской карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации - эмитента банковской карты, не возмещаются.

РЕКОМЕНДАЦИИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С БАНКОВСКОЙ 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 банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.

6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская 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 банковской карты.

9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская 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 банковской картой в банкоматах.

12. Если при проведении операций с банковской картой в банкомате банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты, которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

РЕКОМЕНДАЦИИ ПРИ ИСПОЛЬЗОВАНИИ БАНКОВСКОЙ КАРТЫ ДЛЯ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ И УСЛУГ.

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

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

3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской 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 банковской 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 БАНКОВСКОЙ 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 банковской карте или счете через сеть Интернет, например, ПИН, пароли доступа к ресурсам банка, срок действия банковской 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 банковскую 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 банковской карте или 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.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПУТЕМ ИСПОЛЬЗОВАНИЯ ЛОЖНЫХ (ФАЛЬСИФИЦИРОВАННЫХ) РЕСУРСОВ СЕТИ ИНТЕРНЕТ.

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей ДБО файлов с секретными данными и пароли. Трояны распространяются через e-mail, по каналам сервисов мгновенной передачи информации, через принадлежащие злоумышленникам сайты. При этом злоумышленники похищают персональные данные и пароли доступа, что позволяет совершать операции от имени клиента.

При работе в Интернет с использованием ДБО рекомендуется соблюдать следующие правила безопасности, применяющиеся для защиты данных:

1. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
2. Пользоваться персональными компьютерами с установленным лицензионным программным обеспечением.
3. Своевременно обновлять установленное программное обеспечение и операционную систему (установка критичных обновлений).
4. Включить системный аудит событий операционной системы, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
5. Установить и своевременно обновлять на компьютере антивирусное программное обеспечение (ПО).
6. Антивирусное ПО должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.
7. При выходе в Интернет использовать сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.
8. Не давать разрешения неизвестным программам выходить в Интернет.
9. При работе в Интернет не соглашаться на установку каких-либо дополнительных программ.
10. Воздерживаться от использования программ онлайнового общения на компьютере, использующемся для работы в системе ДБО.
11. Необходимо предусмотреть невозможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.
12. Рекомендуется ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.
13. Важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.
14. Важно знать, что ни одна антивирусная программа не обеспечивает 100% защиты.

В целях обеспечения безопасности необходимо подключить функцию SMS-информирования операций посредством отправки сообщений на сотовый телефон.

Прочие меры:

1. Хорошей практикой является полный отказ от установки новых программ и использования сети Интернет на компьютере, предназначенном для работ в системе ДБО Домашним пользователям можно рекомендовать использование виртуальной машины для просмотра Интернет-сайтов и компьютерных игр.
2. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования систем ДБО до исправления ситуации.
3. Крайне желательно при плановом длительном не использовании системы ДБО блокировать операции в системе до предоставления в Банк письма на бумажном носителе.
4. Следите за своими операциями. Выписка по счетам, полученная через систему ДБО, позволит Вам своевременно обнаружить и оперативно известить Банк об имеющихся несоответствиях.

ТРЕБОВАНИЯ К ПЕРСОНАЛЬНОМУ КОМПЬЮТЕРУ, ИСПОЛЬЗУЕМОМУ ПРИ РАБОТЕ В СИСТЕМЕ ДБО.

Обращаем Ваше внимание, что персональные компьютеры, на которых ведется работа в системе ДБО, должны отвечать следующим требованиям:

1. Пароли учетных записей, обладающих правами администратора, должны быть сложными и содержать не менее 6-ти символов.
2. Пароль доступа необходимо менять не реже одного раза в 3 месяца, или при подозрении в компрометации ключей. В частности, компрометацией является вирусная активность на персональном компьютере в период использования системы ДБО.

3. Учетная запись «Гость» должна быть выключена.
4. Не должно быть учетных записей с пустыми паролями.
5. Обращать внимание на дату и время последних входов в систему.
6. Прежде чем вводить логин и пароль убедитесь, что Вы находитесь на сайте системы ДБО: в адресной строке должен быть адрес **https:\\timerbank.ru.** Будьте внимательны: сайты, выглядящие почти точной копией банковских, созданы специально для получения Ваших персональных данных.
7. Не записывайте свой логин и пароль к системе ДБО там, где он может стать доступным другим лицам.
8. Старайтесь не работать с системой ДБО с общедоступных компьютеров, например, в Интернет-кафе. Если Вам пришлось воспользоваться системой с компьютера общего пользования, поменяйте пароль с личного компьютера при первой же возможности.
9. При подозрении на то, что Ваши данные могли стать известными третьим лицам, незамедлительно обратитесь в Банк по телефону **8-800-100-66-77**.
10. Не отправляйте конфиденциальную информацию о средствах доступа к системе ДБО и/или движении Ваших денежных средств по электронной почте.

Для смены пароля доступа к системе ДБО воспользуйтесь web-интерфейсом системы ДБО. Если Вы обнаружили в сети Интернет ложный Web-сайт «Тимер Банка» (ПАО), отличный от https:\\online.bta-kazan.ru, https:\\www.timerbank.ru, или с Вами пытаются связаться по электронной почте или иным способом лица, с требованиями о предоставлении персональных идентификаторов доступа к системе ДБО, просьба немедленно сообщить об этом в Службу безопасности «Тимер Банка» (ПАО) по телефонам: (843) 525-74-97, 525-74-96.

Просим отнестись с особым вниманием к расчетам в сети Интернет и не отвечать на сомнительного рода запросы. Стоит помнить, что Банк никогда не будет по электронной почте запрашивать персональную информацию клиента. Это противоречит соображениям безопасности.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошеннических действий.