

Меры безопасности по использованию банковских платежных карточек

Общие рекомендации

1. Храните в тайне от других лиц конфиденциальные данные карточки: номер и срок действия карточки, указанный на оборотной стороне трехзначный код проверки подлинности карточки, ПИН-код, который желательно запомнить.

Ни в коем случае нельзя хранить ПИН-код вместе с карточкой, а также записывать его на карточке, в записной книжке мобильного телефона, в паспорте и т.п.

2. **Никогда не сообщайте ПИН-код другим лицам**, включая родственников, знакомых, работников банков, организаций торговли/сервиса, представителей правоохранительных органов. Не передавайте ПИН-код ни по телефону, ни по электронной почте.

3. **Не подвергайте** банковскую карту **механическим, температурным и электромагнитным** воздействиям, а также избегайте попадания на нее влаги, красителей, растворителей, вредных химических веществ.

4. **Храните** карточку в **безопасном, недоступном** для других лиц месте. При использовании Карточки для расчетов за товары (работы, услуги) в ОТС, проведения других операций не упускать Карточку из своего поля зрения.

5. Немедленно **блокируйте** карточку в случае **утери/кражи**, оставлении ее в банкомате или ином устройстве самообслуживания, изъятии кассиром организации торговли/сервиса, ее компрометации (если конфиденциальные данные карточки стали известны посторонним лицам) либо при возникновении подозрений в ее компрометации. Для постоянного контроля над расходными операциями, проводимыми по Вашей карте, рекомендуем Вам подключить услугу банка – «SMS-оповещение».

Если при наличии у Вас подключенной услуги «SMS-оповещение» сообщения от банка о проводимых операциях перестали поступать на Ваш мобильный телефон, необходимо связаться с Банком для уточнения причин.

При получении информационного сообщения о подозрительной операции, которую Вы не совершали, а также, если полученное от банка сообщение вызывает какие-либо сомнения или опасения, например, с просьбой позвонить в банк по указанным в сообщении телефонам, необходимо заблокировать карточку любым из доступных Вам способов и обратиться в службу клиентской поддержки Банка по единому номеру: 306-20-40.

6. Будьте внимательными, отвечая на телефонные звонки и сообщения, поступающие от лиц, представляющих работников банка: если работника банка интересует ваш **ПИН-код, полный номер карточки, срок ее действия** или иные сведения, которые вызывают у Вас подозрения, необходимо прервать звонок и самостоятельно связаться со службой поддержки Банка.

7. Установите ограничения (лимиты) на снятие наличных денежных средств и безналичные операции как на территории Республики Беларусь, так и за ее пределами.

8. Старайтесь регулярно проверять состояние своего счета, а также после заграничных поездок, в которых использовалась карточка. При выявлении расхождений между фактически совершенными и отраженными в выписке операциями обратитесь в Банк для уточнения обоснованности операций.

9. При смене номера вашего контактного телефона, а также паспортных данных, свяжитесь с Банком для актуализации ваших данных.

Снятие наличных денежных средств в банкоматах (АТМ)

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

2. При получении наличных денежных средств в банкоматах, особое **внимание** обратите на **основные элементы банкомата**: картоприемник, ПИН-клавиатуру, устройство для выдачи денежных средств. Обратите внимание на щель картоприемника: мошенники могут установить поверх картоприемника или непосредственно в картоприемник непредусмотренную конструкцией банкомата накладку.

Зачастую мошенники оставляют заметные следы: щели, клеевые подтеки и сколы. Порой мошенники делают поддельные панели с видеокамерами, которые затем крепятся к банкомату: на

диспенсер для денег, под козырек, под экран или даже в стенде для рекламных брошюр. Эти камеры издали могут выглядеть как черные точки.

Если что-либо во внешнем виде банкомата или его работе вызывает у Вас сомнение, или Вы заметили у банкомата дополнительное оборудование или провода, или банкомат поврежден – не используйте этот банкомат и, по возможности, сообщите об этом в Банк.

3. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.

4. Если банкомат не вернул карточку, ее обязательно нужно заблокировать, позвонив по единому номеру: 306-20-40. Для возврата карточки позвоните в банк, которому принадлежит банкомат по телефону, указанному на банкомате.

5. Помните, что в случае трехкратного ввода неправильного ПИН-кода, карточка будет заблокирована. Для разблокировки карточки обратитесь в Банк по единому номеру: 306-20-40.

6. Не оставляйте запрошенный Вами карт-чек в банкомате или другом устройстве самообслуживания, так как в чеке могут быть указаны сумма операции, остаток денежных средств.

Получение наличных денежных средств и проведение операций безналичной оплаты с использованием карточки в отделении банка

1. Все действия работника банка с Вашей карточкой должны проходить под Вашим наблюдением. Не разрешайте работнику Банка уходить с Вашей карточкой в другое помещение.

2. При получении наличных денежных средств либо проведении безналичной оплаты особое внимание обращайте на **соответствие** указанной Вами **суммы и валюты операции** сумме и валюте, содержащейся в карт-чеке.

3. Работник Банка вправе потребовать у Вас предъявление документа, удостоверяющего личность (паспорта), для идентификации держателя карточки и оформления операции.

4. При проведении операций в пунктах выдачи наличных обращайтесь особое внимание на действия работника банка, если он пытается провести Вашу карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение несанкционированных операций. Обязательно поинтересуйтесь причиной, по которой работнику необходимо повторно провести карточку через считывающее устройство оборудования.

5. Старайтесь не показывать и ни при каких обстоятельствах не сообщать ПИН-код работникам Банка.

Использование банковской карты для безналичной оплаты товаров и услуг

1. В любой торговой или сервисной точке карточка должна обслуживаться **в Вашем присутствии**. Вы должны видеть карту на протяжении всего времени совершения операции.

2. Работники торговой или сервисной точки могут запросить у Вас ввести ПИН-код при оплате товаров и услуг. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости от Вас, не смогут его увидеть.

3. Перед вводом ПИН-кода убедитесь, что сумма и валюта совершаемой операции верны.

4. В случае отказа от покупки требуйте отмены операции. Обязательно сохраняйте карт-чек по операции отмены до момента сверки выписки по счету, к которому выпущена карточка.

5. Для возврата ранее приобретенного товара/услуги предъявите работнику торговли карточку для проведения операции «возврат» и оформления соответствующего документа (чек или слип с отметкой «возврат»). Обязательно сохраните чек возврата. В том случае, если сумма операции не поступит на Ваш счет в течение 30 дней со дня возврата, оформите претензию в письменном виде.

Проведение операций безналичной оплаты с использованием карточки в сети Интернет

1. Для оплаты товаров в сети Интернет лучше **использовать отдельную карточку** (к отдельному счету и с ограниченной суммой денежных средств на нем), предназначенную только для данной цели. Совершайте покупки только в тех интернет-магазинах, которые вызывают у вас доверие.

2. Не отвечайте на электронные письма, в которых от имени банка или иных организаций, а также граждан Вас просят предоставить персональную информацию, в том числе реквизиты Вашей карточки, в целях их обновления или для регистрации.

3. Злоумышленники часто распространяют вирусные программы через различные интернет-

ресурсы, посредством электронной почты, программ обмена сообщениями. Клиент, компьютер которого заражен, при попытке войти в личный кабинет может незаметно перенаправляться на «фишинговый» сайт, который внешне практически не отличается от подлинных сайтов интернет-банков. Чтобы этого избежать, старайтесь максимально использовать возможности вашего браузера и почтового клиента по обеспечению безопасности. Для этого в опциях браузера и почтового клиента необходимо включить дополнительные функции. Например, «Блокировка всплывающих окон», «Защита от фишинга и вредоносного ПО», «Открывать файлы на основе содержимого, а не расширения» и др. Также не стоит пользоваться окном предварительного просмотра в используемом Вами почтовом клиенте. Кроме того, рекомендуется всегда самостоятельно вводить веб-адрес Банка (интернет-банкинга) в адресную строку браузера вместо использования любых гиперссылок, тем более из подозрительных сообщений.

4. Проверяйте **правильность адресов интернет-сайтов**, к которым подключаетесь для совершения покупки, так как похожие адреса могут использоваться для осуществления неправомерных действий.

5. Внимательно читайте условия совершения операций, связанных с **азартными играми** (казино, лотереи), а также с **подписками** в сервисах (такси, маркетплейсы и т. п.). Некоторые операции могут автоматически активировать платную подписку, что приведет к регулярному списанию средств с вашей карты.

6. **Сохраняйте** любые **электронные документы**, переписку по электронной почте, касающуюся попыток разрешения спорной ситуации с организацией торговли/сервиса, так как эти сведения могут оказаться важны для защиты Ваших прав потребителя. При невозможности самостоятельно разрешить спорную ситуацию обратитесь в Банк. Если условия для Вас непонятны, откажитесь от платежа. Помните, что возврат денежных средств по совершенным Вами операциям возможен далеко не во всех случаях.

7. Не стоит позволять браузерам сохранять данные карточки для упрощения совершения покупок в будущем.

Особенности проведения операций с использованием карточки

1. Необходимо учитывать, что специфика совершения операций с использованием карточки предполагает наличие **временного разрыва** между датой совершения операции и отражением данной операции по счету. Продолжительность периода между днем совершения операции и днем отражения операции по счету зависит от места осуществления операции (на территории Республики Беларусь или за границей), времени осуществления операции (ночное или дневное время, рабочие или выходные, праздничные дни).

2. Если вы все же пострадали от мошенничества: необходимо немедленно обратиться в службу клиентской поддержки Банка, для блокировки карточки и следовать рекомендациям специалиста. По факту мошенничества рекомендуется подать заявление в правоохранительные органы.

3. При оплате товаров/услуг за границей стоит обращать внимание на наличие сервиса **Dynamic currency conversion (DCC)**, что в переводе означает «динамический обмен валюты». Этот сервис предлагает дополнительный этап конверсии, что, как правило, приводит к уплате дополнительной комиссии: сумма к оплате пересчитывается в белорусские рубли по курсу, установленному банком, предлагающим услугу DCC. Необходимо внимательно следить за информацией, представленной на экране терминала (в частности, стоит обращать внимание на наличие аббревиатуры DCC). В случае несогласия с условиями проведения операции не подтверждайте ее вводом ПИН-кода, настаивайте на отмене операции и ее проведении без применения динамической конверсии.

Использование систем дистанционного банковского обслуживания

1. Не забывайте периодически (а также в случае, если пароль стал известен посторонним лицам) **менять свой пароль**. Старайтесь сделать его максимально сложным и уникальным. Для этого используйте в пароле прописные и строчные буквы, цифры и символы. Не используйте один и тот же пароль в разных системах (электронная почта, системы интернет-банкинга других банков, социальные сети и т. п.). Постарайтесь избегать в пароле даты своего рождения, имени и других доступных о вас данных. Не разглашайте свой пароль никому, включая сотрудников банка.

2. По окончании сеанса работы с системой интернет-банкинга обязательно выходите из системы, используя соответствующую опцию.

Мобильный банкинг

1. Устанавливайте мобильные приложения только из известных источников (Google Play Market, App Store, AppGallery).
2. Необходимо использовать мобильные устройства с работающими системами защиты, такими как: ограничение доступа к устройству, активное антивирусное программное обеспечение с обновленными базами данных, система обновления операционной системы.
3. При утрате мобильного телефона/устройства, на котором установлено мобильное приложение Банка или неожиданным прекращением работы SIM-карты, следует как можно быстрее заблокировать SIM-карту.
4. Никогда не оставляйте открытым мобильное приложение: всегда пользуйтесь кнопкой для завершения работы.

Недопустимость использования карточки третьими лицами

Не передавайте третьим лицам карточку и не позволяйте третьим лицам использовать реквизиты карточки. Не позволяйте третьим лицам рассматривать карточку и (или) записывать (копировать, снимать и т.п.) какие-либо данные, нанесенные на карточку.