Меры безопасности

Общие рекомендации

1. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
При отсутствии подписи на карточке либо несоответствии подписей на карточке и карт-чеке держателю карточки может быть отказано в проведении операции с ее использованием.

2. Храните втайне 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 картой в кошельке, а также записывать его на карте, в записной книжке мобильного телефона, в паспорте и т.п. Помните – если Карта будет украдена вместе с сумкой, вор непременно отыщет ПИН-код, и, имея его, беспрепятственно сможет израсходовать все имеющиеся на карте деньги.
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. 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, красителей, растворителей, вредных химических веществ. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.

4. Помните, что карту необходимо хранить и беречь также, как наличные деньги, поэтому не оставляйте ее без внимания в местах, где она может стать легко доступной посторонним лицам (например, в машине, в местах массового отдыха, в отеле, на пляже и т.п.). **Учтите, что в случае, если Вашу карту использует кто-либо из Ваших близких или друзей, Вы будете ответственным за эти сделки!**

5. Запишите номер **+375 (29) 270-00-00** в записную книжку мобильного телефона. Немедленно блокируйте Карту в случае утери/кражи, а также подозрения в проведении по карте мошеннических операций. Для постоянного контроля над расходными операциями, проводимыми по Вашей карте, настоятельно рекомендуем Вам подключить услугу банка – «SMS оповещение». Чем быстрее Вы позвоните, тем выше вероятность того, что деньги на Вашей карте останутся нетронутыми.
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, необходимо заблокировать карточку любым из доступных Вам способов и обратиться в службу клиентской поддержки Банка.

6. При обнаружении утери/кражи карточки, 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 необходимо немедленно заблокировать карточку и обратиться в Банк.

7. При получении сообщения с просьбой позвонить в банк по указанным в сообщении телефонам рекомендуется связаться со службой поддержки клиентов Банка по номеру **306-20-40** или **+375 (29) 270-00-00** и сообщить о факте получения такого сообщения.
Также будьте внимательными, отвечая на телефонные звонки и сообщения, поступающие якобы от банка: если работника банка интересует ваш ПИН-код, **полный** номер карточки, срок ее действия или что-то, что вызывает у вас подозрения, необходимо прервать звонок и самостоятельно связаться со службой поддержки Банка.

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

9. 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.

10. При смене номера вашего контактного телефона, свяжитесь с Банком для актуализации ваших данных.

Снятие наличных 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 в банкоматах, во избежание несанкционированного копирования магнитной полосы Карты и ПИН-кода, будьте внимательнее.
Особое **внимание** обратите на **основные элементы банкомата**: картоприемник, ПИН-клавиатуру, устройство для выдачи денежных средств. Особое внимание обратите 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. Лучше не использовать банкомат, картоприемник которого выглядит так, будто кто-то ковырял его отверткой или облил клеем.
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 издалека 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. Никогда не принимайте помощи посторонних лиц при пользовании банкоматом. Убедитесь, что окружающие (в т.ч. стоящие в очереди у банкомата), не видят клавиш, которые Вы используете для ввода ПИН-кода.

В случае затруднений, возникших при использовании карточки, не прислушивайтесь к советам посторонних лиц.

5. Если банкомат не возвратил Карту, ее обязательно нужно заблокировать, позвонив в будние дни с 8.30 до 17.30 по телефону **+375 (17) 306-20-40**, а в остальное время, выходные и праздничные дни круглосуточно по телефону **+375 (29) 270-00-00**. Для возврата карты позвоните в банк, которому принадлежит банкомат по телефону, указанному на банкомате.

6. Помните, что в случае трехкратного ввода неправильного ПИН-кода, карта будет заблокирована. Для разблокировки карты обратитесь в Банк по номеру **+375 (17) 306-20-40.** Помните, что ПИН-код не подлежит восстановлению. Если Вы забыли ПИН-код карты, обратитесь в любое отделение Банка для перевыпуска карты.

7. В случае если банкомат или другое устройство самообслуживания работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого устройства, отменить совершаемую операцию, нажав на клавиатуре соответствующую кнопку, и дождаться возврата карточки. Если устройство не возвращает карточку, следует незамедлительно заблокировать карточку любым доступным Вам способом и обратиться в Банк.

8. 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 предъявления документа, удостоверяющего личность (паспорта), для идентификации держателя карточки и оформления операции.

4. При проведении операций в пунктах выдачи наличных обращайте 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 карта должна обслуживаться **в Вашем присутствии**. Вы должны видеть карту на протяжении всего времени совершения операции.

2. У работников торговли есть право запросить у Вас удостоверяющий личность документ, а также 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. Убедитесь, что работник торговли уничтожил ранее оформленный чек (слип). 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 карту 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 и передайте её в Банк вместе с чеком возврата.

6. Перед оплатой за товары или услуги в устройствах самообслуживания организаций торговли/сервиса (например, на автозаправочной станции) изучите имеющуюся информацию о правилах совершения платежей, размещенную на экране устройства или рядом с ним, и следуйте инструкциям системы самообслуживания.

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. Постарайтесь выяснить правомерность таких предложений, связавшись с Банком.

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. Если у Вас появились какие-либо подозрения относительно интернет-страницы или Вы не хотите предоставлять персональные данные или данные карточки, то покиньте страницу и совершите покупку в другом месте.

5. Перед совершением операции оплаты товара/услуги внимательно изучите условия предлагаемого соглашения, в частности, все правила предоставления услуг, условия доставки, возврата, замены товара, а также процедуру отмены заказа. Особенно внимательно читайте условия совершения операций, связанных с азартными играми (казино, лотереи), так как они могут предусматривать автоматическую подписку, что повлечет списание денежных средств на регулярной основе.

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. Если Вами было произведено бронирование гостиницы через интернет-сайт, но по каким-то причинам Вы не планируете воспользоваться ею, обязательно проведите отмену бронирования через тот же интернет-сайт согласно указанным на нем процедурам.
Получение Вами кода отмены бронирования отеля является доказательством того, что бронь действительно отменена. В ином случае за несвоевременную отмену брони гостиница имеет право представить к списанию с Вашего счета сумму денежных средств в установленном ею размере.

8. Никогда **не сообщайте свой ПИН-код** при заказе товаров по телефону или почте и не вводите его в форму заказа на сайте торговой точки. При совершении удаленных операций ввод ПИН-кода никогда не требуется.

9. Совершайте покупки только со своих устройств, не пользуйтесь интернет-кафе и другими общедоступными средствами, где могут быть установлены программы-шпионы, запоминающие Ваши конфиденциальные данные.

10. Устанавливайте на свои устройства лицензионное программное обеспечение, в том числе антивирусное, межсетевые экраны (фаерволы/брандмауэры), и регулярно производите их обновление. Это поможет защитить Ваши устройства от вирусов и других деструктивных программ, а также от несанкционированного доступа к Вашим конфиденциальным данным.

11. 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. В зависимости от страны пребывания при проведении операции с использованием карточки **может удерживаться дополнительная комиссия**, о размерах которой целесообразно поинтересоваться у обслуживающего вас работника перед совершением операции. Также такая информация может быть отображена на экране банкомата или устройства самообслуживания при совершении операции.

3. При проведении операций без вашего физического присутствия во время и (или) в месте проведения оплаты (например, посредством почты, факса, телефона и т. п.) сообщайте (вносите в соответствующие поля) необходимые реквизиты карточки только для проведения операции, которую вы сами инициировали и считаете правомерной.

4. 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.

5. 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. При использовании интернет-банкинга обращайте внимание на наличие на странице сервиса защищенного протокола HTTPS. Перед входом в систему рекомендуется **удостовериться в подлинности сертификата и сайта**. Для этого необходимо кликнуть в поле адресной строки Интернет (как правило, это поле с пиктограммой замка или листа бумаги) и сверить имеющуюся в блоке информацию. При несоответствии данных с реальными сведениями о банке стоит покинуть страницу.

2. 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.

3. Будьте осторожны, посещая сайты с сомнительным содержанием: именно они, как правило, являются источником самых новых вирусов, работа которых может быть направлена на хищение ваших данных (в том числе, логинов и паролей).

4. 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, Windows Store, App Store).

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. Не устанавливайте мобильное приложение Банка на мобильный телефон/устройство, на котором получены root-права (права суперпользователя). Такие телефоны и устройства также не рекомендуется использовать для получения сообщений от банка (например, SMS с кодом (одноразовым паролем) для прохождения аутентификации).

4. При утрате мобильного телефона/устройства, на котором установлено мобильное приложение Банка или неожиданным прекращением работы SIM-карты, следует как можно быстрей заблокировать SIM-карту.

5. Никогда не оставляйте открытым мобильное приложение: всегда пользуйтесь кнопкой для завершения работы.