Рекомендации относительно необходимых мер безопасности

 Прочтите Правила пользования карточкой, предоставленные Вам банком. Свяжитесь с сотрудниками банка, если какие-либо Правила Вам непонятны.

 При получении в Банке карточек обязательно проставьте на них в соответствующем месте образец личной подписи.

 Никогда не оставляйте свою карточку без присмотра, храните ее в безопасном месте.

 Оплачивая покупки платежной карточкой, старайтесь, чтобы все операции по ней совершались в Вашем присутствии. Не разрешайте продавцу/официанту уносить Вашу карточку в другое помещение, требуйте, чтобы операции проводили в Вашем присутствии.

 Если Вы отказались от покупки, или если при оформлении чека или слипа были допущены ошибки, попросите, чтобы испорченный чек/слип уничтожили в Вашем присутствии, а второй экземпляр заберите с собой и храните в течение месяца (до сверки с выпиской по карточному счету).

 По мере возможности не используйте Вашу карточку в Интернете, не передавайте реквизиты Вашей карточки (номер карточки, специальный код CVC2 – Card Verification Code 2 , срок действия) по электронной почте.

 Для проведения операций в глобальной сети Интернет, рекомендуем использовать карточку VISA VIRTUON, она значительно уменьшит риск мошеннических транзакций при оплате товаров и услуг.

 Никогда не записывайте ПИН-код (персональный идентификационный номер) на карточке. ПИН-код следует запомнить. Если же Вы все-таки решили записать ПИН-код, лучше это сделать в зашифрованном виде, чтобы он не мог стать известен кому-либо, кроме Вас, и никогда не носите его вместе с карточкой.

 Никогда не раскрывайте свой ПИН-код, Вы никому не обязаны его сообщать: ни сотрудникам банка, ни представителям правоохранительных органов, ни кассирам торговых точек. Только держатель карточки должен знать свой ПИН-код.

 В случае утери или кражи карточки, необходимо незамедлительно обратиться в банк или в Контакт-Центр, для того, чтобы сотрудники банка осуществили блокирование карточки, во избежание мошенничества по ней.

 Никогда не передавайте свою карточку третьим лицам: другу, супруге, особенно если они едут за границу. Если банкомат по какой-либо причине изымет карточку, то у Вас и у Ваших близких могут возникнуть проблемы.

 Контролируйте пользование дополнительными карточками членами Вашей семьи. Вы несете полную ответственность по всем операциям, произведенным по дополнительным карточкам.

 Регулярно проверяйте выписку по счету. Чем быстрее Вы обнаружите и сообщите Ваши подозрения о сомнительных операциях, тем лучше. Для выставления претензий существуют строго оговоренные сроки, в течение которых Вы и банк сможете что-то предпринять. Сохраняйте чеки и сверяйте их с выпиской по счету карточки. Чаще проверяйте остаток по Вашему карточному счету.

 Вы можете обратиться в банк за установлением ежедневного или ежемесячного лимита расходования по Вашему усмотрению. Это дополнительно обезопасит Ваш счет от мошенничества.

 В случае получения электронного сообщения от банка, с просьбой сообщить какие-либо персональные данные, немедленно свяжитесь с банком по уже известному Вам номеру телефона и убедитесь в действительности отправления такого сообщения банком.

 В случае возникновения подозрений о том, что реквизиты Вашей карточки стали известны посторонним лицам, незамедлительно сообщите об этом в свой банк.

1. МЕРЫ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ОПЕРАЦИЙ ЧЕРЕЗ БАНКОМАТ:

 При получении наличных средств в банкомате, Вам необходимо убедиться, что банкомат обслуживает карточки нужной Вам платежной системы (обычно на банкоматах располагаются наклейки, информирующие клиентов о том, карточки каких платежных систем обслуживаются банкоматом).

 Перед проведением операции через банкомат, необходимо оценить обстановку. Увидев какие-либо внешние признаки неисправности банкомата, обнаружив рядом с ним или на нем, посторонние устройства, сообщите об этом в банк и воспользуйтесь другим банкоматом.

 Не пользуйтесь теми банкоматами, на экране которых отражается сообщение с просьбой о переходе на другие банкоматы. Банки не помещают подобные сообщения.

 Во всех случаях, насколько это возможно, пользуйтесь банкоматами, с которыми Вы уже знакомы. В других случаях, выберите банкоматы в хорошо освещенных и удобных местах расположения.

 Если Вы собираетесь воспользоваться банкоматом, находящемся в специальном помещении, откройте дверь помещения своей карточкой, поместив ее в устройство доступа. Данные устройства не должны требовать ввода ПИН-кода. Если Вы обнаружите устройство доступа в помещение, требующие ввода ПИН-кода, не пользуйтесь им.

 Убедитесь в том, что люди, стоящие за Вами в очереди, не имеют возможности подсмотреть Ваш ПИН-код. Закрывайте от посторонних клавиатуру банкомата рукой при вводе своего ПИН- кода.

 Если вы чувствуете, что банкомат функционирует неправильно, нажмите кнопку «Отмена», заберите карточку и воспользуйтесь другим банкоматом.

 Никогда не применяйте силу, чтобы вставить карточку в карточный слот (прорезь приемного устройства).

 Не позволяйте никому отвлечь Вас, когда находитесь у банкомата.

 Заберите наличные и карточку после завершения операции. Не пересчитывайте полученные деньги около банкомата – сразу уберите наличные, карточку и чек.

 Если случилось так, что Ваша карточка застряла в банкомате, остерегайтесь людей, предлагающих помощь Вам в этот момент. Следует немедленно сообщить об этом в свой банк для блокирования Вашей карточки, а также к персоналу отделения банка, если банкомат расположен в отделении.

2. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ ВИДЫ МОШЕННИЧЕСТВА:

Фишинг Рассылка пользователям сети Интернет электронных писем от имени банка-эмитента, с просьбой уточнить данные по платежным карточкам, либо содержащие ссылку на сайт банка, который держателю карточки необходимо посетить. На сайте им предлагают ввести личные данные, якобы потерянные из-за технического сбоя системы: номер кредитной карточки, идентификатор, пароль и иногда даже ПИН-код. После этого финансовые средства со счетов платежной карточки могут использоваться мошенниками через интернет-магазины. Bank RBK НИКОГДА НЕ ЗАПРАШИВАЕТ Вашу персональную информацию по электронной почте, т.к. это противоречит соображениям безопасности. Пожалуйста, обращайте внимание на сообщения о подозрительных операциях. Так, если

Вам сообщают, что на Ваш счёт поступили деньги, которых Вы не ожидали, этого достаточно, чтобы заподозрить попытку мошенничества. Если Вы всё же успели стать жертвой мошенников или подозреваете, что Ваши данные попали в чужие руки, рекомендуем Вам незамедлительно сообщить об этом в АО «Bank RBK».

Неэлектронный фишинг Это «новая услуга» - получение наличных денежных средств на предприятиях торговли. При получении денежных средств держателя просят набрать свой ПИН-код, правильность набора которого должен проверить банк-эмитент. Но ПИН-код не направляется эмитенту, а записывается мошенниками с помощью устройства, имитирующего ПИН-ПАД (дополнительный модуль торгового терминала, специально предназначенный для набора ПИН-кодов и обеспечения их конфиденциальности). Держатель карточки лишь через некоторое время может обнаружить в выписке по счету своей платежной карточки операции снятия наличных денег в банкоматах, которые он не совершал.

Скимминг Существуют специальные виды электронных устройств, которые при установке на банкоматах позволяют считывать и фиксировать как реквизиты карточки (номер карточки, специальные параметры), так и ПИН-код. Подобные устройства хитро замаскированы под обычные части банкомата. Считывающее устройство накладывается поверх гнезда для ввода карточки, поверх клавиатуры или используются миниатюрные видеокамеры, замаскированные под ящичек с информационными/рекламными брошюрами.