РЕКОМЕНДАЦИИ

по безопасному использованию пластиковой карты

1. После получения карты поставьте шариковой ручкой свою подпись на специальной полосе для подписи, расположенной на оборотной стороне карты. При отсутствии подписи карта может быть не принята к оплате в торгово-сервисном предприятии, а также повышается риск использования карты злоумышленниками в случае ее утраты/кражи.
2. Храните свою карту в недоступном для окружающих месте. Не передавайте карту другому лицу, в том числе родственникам и знакомым, за исключением продавца (кассира) для проведения транзакций. Рекомендуется хранить карту отдельно от наличных денег и документов, особенно в поездках.
3. Во избежание мошенничества с использованием Вашей карты требуйте проведения операций с картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения с целью исключения потерь от несанкционированного использования Вашей карты (копирования информации с магнитной полосы Вашей Карты для дальнейшего мошеннического ее использования).
4. Не забывайте забрать Вашу карту после проведения операции. Убедитесь, что возвращенная карта принадлежит Вам. Запрещается оставлять под любым предлогом карту в организациях торговли (услуг).
5. Проверяйте правильность суммы, указанной на платежном чеке. Поставив подпись на платежном чеке, Вы соглашаетесь со списанием указанной на нем суммы с Вашего карточного счета. Не используйте карту для оплаты, если кассир или торговая точка не вызывают у Вас доверия. Особенно осторожно используйте карту в странах повышенного риска (Малайзия, Таиланд, Сингапур, Тайвань, Филиппины, Турция, Мексика, Австралия, Венесуэла, Гонконг, Индонезия, Украина) В этих странах высок риск копирования данных Вашей карты и использования их для изготовления подделок. В таких странах для снятия наличных денежных средств рекомендуется использовать банкоматы известных банков, которые установлены в отделениях и крупных торговых центрах.
6. Обязательно сохраняйте все документы по операциям до момента отражения в выписке по Вашей карте.
7. Не принимайте помощь третьих лиц, а также не прислушивайтесь к советам посторонних людей при проведении операций, особенно при снятии наличных денежных средств в банкоматах. При необходимости обратитесь к работникам в Банке или позвоните по телефонам, указанным на банкоматах или на оборотной стороне Вашей карты.
8. Во избежание использования Вашей карты третьим лицом храните ПИН-код отдельно от карты, исключив одновременный доступ к ним, не пишите ПИН-код на карте, не сообщайте ПИН-код другим лицам (в том числе родственникам), при опросах/ информировании по телефону, электронной почте и т.д. в том числе лицам, представляющимися сотрудниками Банка, не вводите ПИН-код при совершении операций в сети Интернет.
9. Для контроля операций по Вашей карте в режиме реального времени и своевременного выявления несанкционированных операций рекомендуем Вам подключить услугу SMS-банк.
10. В случае смены номера телефона, утраты сим-карты, обязательно обратитесь в Банк для отключения sms-оповещения от прежнего номера телефона.
11. Во избежание порчи магнитной полосы не держите карту в непосредственной близости от источников электромагнитного излучения (дисплеев, телевизоров, СВЧ-печей, аудио и видео аппаратуры и т.д.). Не подвергайте Вашу карту тепловому воздействию. Не допускайте механического воздействия (не сгибайте и не царапайте) на карту, помните, что карта изготовлена из пластика.

Помните! Передача банковской карты или ее реквизитов, идентификаторов и паролей, предназначенных для доступа и подтверждения операций в сети Интернет, другому лицу означает, что Вы предоставляете возможность другим лицам проводить операции по Вашим счетам.

Внимание! Если Вы получили СМС-сообщение от Банка по операции, которую Вы не совершали, необходимо срочно заблокировать карту, позвонив по телефонам, указанным на оборотной стороне Вашей карты.

При любых подозрениях на мошенничество, следует так же незамедлительно обратиться в Сервисную службу или к специалистам Банка по телефонам:

**8-800-200-4575 (круглосуточно)**

**8-3466-41-26-09**

**8-3466-41-26-55**

Запишите указанные номера в память Вашего телефона, чтобы оперативно обратиться в Сервисную службу или к специалистам Банка при необходимости.

Подробная информация о способах мошенничества и мерах защиты размещена на сайте АО КБ «Приобье» - [**www.priobye.ru**](http://www.priobye.ru)

**Меры безопасности при работе в системе «FAKTURA.RU»**

Для входа в личный кабинет «FAKTURA.RU» Вам необходимо ввести логин и пароль. Для входа в систему «FAKTURA.RU» не требуется вводить никакой другой информации.

Внимание! Если для входа в «FAKTURA.RU» Вам предлагается ввести любую другую персональную информацию или дополнительные данные (номер мобильного телефона, контрольную информацию по банковским картам или другие данные), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в системе «FAKTURA.RU» и срочно обратиться в Банк.

Банк никогда не запрашивает пароли для отмены операций в системе «FAKTURA.RU». Если Вам предлагается ввести пароль для отмены операции, в том числе и той, которую Вы не совершали, Вам необходимо прекратить сеанс работы в системе «FAKTURA.RU» и срочно обратиться в Банк.

Ни при каких обстоятельствах не сообщайте свои пароли никому, включая работников

Банка.

При работе с услугой «FAKTURA.RU» всегда проверяйте, что установлено защищенное ssl- соединение с официальным сайтом. В окне браузера должно быть изображение, обозначающее наличие защищенного соединения, которое отличается в зависимости от браузера. Например, в браузере Microsoft Internet Explorer версия 8.0 в правой части адресной строки располагается желтый замочек, в более ранней версии - его изображение находится в правом нижнем углу экрана.

Для исключения компрометации Вашей финансовой информации и хищения средств, настоятельно не рекомендуется подключать к услугам Банка корпоративные номера телефонов и номера, которые Вам не принадлежат, в том числе по рекомендации третьих лиц, представившихся работниками Банка.

Не устанавливайте на мобильный телефон или иное устройство, на которое Банк отправляет СМС- сообщения с подтверждающими одноразовыми паролями, приложения по ссылкам, полученным от неизвестных Вам источников.

Внимание! На смартфонах и иных устройствах, подключенных к «FAKTURA.RU», Банк НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТ использовать антивирусные программы, доступные в магазинах мобильных приложений, в том числе бесплатно.

Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через СМС/MMS/e-mail - сообщения.

На компьютерах, которые Вы используете для работы в «FAKTURA.RU»:

* используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;
* своевременно устанавливайте обновления операционной системы, рекомендуемые компанией- производителем;
* используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты вашего устройства - персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ» - рассылок и пр.;
* Завершение работы с системой выполняйте путем выбора соответствующего пункта меню.

**Меры безопасности при работе с мобильным приложением «FAKTURA.RU» для смартфонов и планшетных устройств**

Рекомендуется установить на телефоне/смартфоне пароль для доступа к устройству, данная возможность доступна для большинства современных моделей устройств.

При утрате мобильного телефона или иного устройства, подключенного к услугам Банка, следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Сервисную службу Банка для приостановки действия услуг, оформить заявление на отключение старого номера телефона и на подключение услуги на новый номер телефона.

При внезапном прекращении работы SIM-карты необходимо обратиться к своему оператору сотовой связи за уточнением причин - в отношении Вас возможно проведение мошеннических действий третьими лицами.

Используйте только официальное мобильное приложение «FAKTURA.RU» (разработчик JSC Center of Financial Technologies), доступное в официальных магазинах приложений производителей мобильных платформ.

Своевременно устанавливайте доступные обновления операционной системы и приложений на Ваш телефон/устройство.

Внимание! На смартфонах и иных устройствах, подключенных к услугам Банка, НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ использовать антивирусные программы, доступные в магазинах мобильных приложений, в том числе бесплатно.

Не устанавливайте на свой телефон/устройство нелицензионные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате Ваш телефон становится уязвимым к заражению вирусными программами.

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

Завершайте работу с мобильным приложением через соответствующий пункт меню.

**Меры безопасности при работе с банкоматами**

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.

* Замки доступа по картам в специальные помещения, где устанавливаются УС, не должны требовать ввода ПИН-кода. Если для прохода в помещение от Вас требуется ввести ПИН-код, не делая этого, обратитесь в Банк. Если Вы ранее пытались воспользоваться подобным устройством, рекомендуем Вам срочно заблокировать карту, обратившись в Сервисную службу или к сотрудникам Банка по указанным телефонам, независимо от того, получили ли Вы доступ к банкомату или нет.
* До проведения операции в банкомате осмотрите его лицевую часть, в частности, поверхность над ПИН- клавиатурой и устройство для приема карты в банкомате. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств, просим незамедлительно сообщить об этом работникам Банка, обслуживающим банкомат, или по телефонам, указанным на банкомате или на оборотной стороне Вашей карты. Операцию с использованием карты для получения наличных в банкомате в данном случае не проводить.
* Не применяйте физическую силу, чтобы вставить банковскую карту в устройство. Если карта не вставляется, воздержитесь от использования такого банкомата.
* При приеме и возврате карты устройством не пытайтесь ускорить прерывистое движение карты в картоприемнике. Неравномерное движение карты является не сбоем, а необходимым средством защиты Вашей карты от компрометации.
* Помните, что карту и деньги необходимо извлечь сразу же после завершения операции. Если карта или/и деньги остаются в приемном устройстве более 30 секунд, банкомат может их удержать.
* Получив деньги, немедленно уберите их в бумажник и не забудьте забрать чек и карту.

Внимание! Не совершайте на банкомате 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 банкомата.

**Меры безопасности при операциях с использованием карты**

**в сети Интернет.**

* Избегайте осуществления Интернет-операций с использованием карты в местах, где услуги Интернет являются общедоступными, например в Интернет-кафе.
* Старайтесь пользоваться проверенными интернет-магазинами, в надежности которых Вы уверены.
* При оплате покупок в сети Интернет Вас попросят ввести код безопасности CVV2. CVV2 - трехзначный код, нанесенный в правой части полосы для подписи, справа от последних четырех цифр номера карты. Этот код вводится для повышения безопасности Интернет-операций с использованием карт.
* Не сообщайте реквизиты Вашей банковской карты (номер карты, срок действия, трехзначный код безопасности (CVV2), нанесенный на полосе для подписи), за исключением использования Вами автоматизированных систем MOTO и систем интернет-коммерции.

**Помните! Надежный интернет-магазин предлагает проведение платежа с использованием сертифицированных средств защиты информации: протокола SSL (Secure Socket Layer) или стандарта SET (Secure Electronic Transaction). Эта информация отражается в правом нижнем углу экрана. Не сообщайте ПИН-код карты при совершении операций в сети Интернет.**

**Защита от СМС и e-mail мошенничества.**

Мошеннические СМС-сообщения, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в СМС-сообщении номер телефона для уточнения информации. Затем мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п., в зависимости от содержания СМС-сообщения.

В случае получения подобных СМС-сообщений настоятельно рекомендуем Вам:

* не перезванивать на номер телефона, указанный в СМС-сообщении;
* не предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, ПИН- коде, CVV2 коде, контрольной информации по карте), или об одноразовых паролях, в т.ч. посредством направления ответных СМС-сообщений;
* не проводить через банкоматы и иные устройства самообслуживания никакие операции по инструкциям, полученным по телефону.

В ряде случаев Банк рассылает информационные СМС-сообщения, при этом:

* в СМС-сообщениях, направляемых Банком по операциям, проведенным с использованием Вашей карты, обязательно указываются последние 4 цифры номера Вашей карты (мошенникам они не известны);
* СМС-сообщения Банка отправляются только от «Faktura.ru», в них указываются только официальные телефоны Банка, опубликованные на официальном сайте или указанные на оборотной стороне Вашей банковской карты.

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

Мошеннические e-mail-рассылки, маскируясь под письма от Банка, как правило, предназначены для заманивания получателей сообщений на сайты - «ловушки», на которых под различными предлогами мошенники попытаются получить персональные данные (логин и пароль для входа в систему «FAKTURA.RU», контрольную информацию по банковским картам, номера банковских карт, ПИН- коды, CVV и иную информацию) или принуждения под различными предлогами на открытие файла - вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла. Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц.

Признаки того, что e-mail-сообщение является мошенническим:

* сообщения замаскированы под официальные письма Банка и требуют от Вас каких-либо быстрых действий или ответа;
* адрес отправителя и тема сообщения замаскированы под обращения от имени Банка. Например:

Примеры тем сообщений в мошеннических

рассылках:

* «Сообщение об увеличении задолженности»
* «Сообщение об увеличении долга»
* «Сообщение об увеличении задолженности на «ДД.ММ.ГГГГ»
* Другие варианты
* письма могут содержат ссылки на Интернет-сайт, похожий на официальный сайт Банка;
* URL-адрес ссылки в письме отличается от официального адреса [(www.priobye.ru)](http://(www.priobye.ru)), возможно также появление всплывающих окон на официальном сайте, в котором запрашивается ввод или подтверждение Ваших персональных данных;
* к сообщению прилагается файл-вложение, который Вам настойчиво рекомендуют открыть;
* в тексте содержатся явные опечатки или орфографические ошибки.

**Обращаем Ваше внимание, что АО КБ «Приобье» никогда:**

* 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 «Faktura.ru» по ссылкам в письмах.

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

1. Необходимо немедленно обратиться по телефонам, указанным на оборотной стороне Вашей карты, для блокировки карты, реквизиты которой были сообщены посторонним или по которой были совершены несанкционированные операции.
2. По факту мошенничества рекомендуется подать заявление в правоохранительные органы.