Безопасность оплаты банковской картой

Оплата по банковским картам на сервисе ООО «FINTECH DRIVE» обрабатывается через платежный шлюз банка АО «Uzum Bank». Данные вашей карты защищены в соответствии со стандартом PCI DSS. Ввод реквизитов карты выполняется на защищенной платежной странице банка, передача информации осуществляется по протоколу SSL с использованием шифрования.

Дальнейшая передача данных производится по закрытым банковским сетям с высоким уровнем надежности.

Для дополнительной аутентификации держателя карты используются протоколы 3D Secure (например Visa Secure, Mastercard Identity Check и др.). Если банк-эмитент поддерживает эту технологию, вы можете быть перенаправлены на его страницу для ввода дополнительного кода подтверждения. В отдельных случаях аутентификация может проходить автоматически на стороне банка без вывода отдельной страницы.

13 правил безопасной оплаты картой

1. Никому и никогда не сообщайте полные реквизиты своей карты, пин-код и код CVV2/CVC2, особенно по телефону или в мессенджерах. Банк может запросить только номер карты (полностью или последние 4 цифры), но не пин-код и не CVV2/CVC2. Для интернет-платежей пин-код не используется.
2. Осторожно относитесь к незнакомым сайтам с подозрительным адресом, отсутствием отзывов и слишком низкими ценами. Такие признаки могут говорить о фишинговом ресурсе.
3. Используйте антивирус и регулярно обновляйте операционную систему и программы. Обновления закрывают уязвимости, которые могут использовать злоумышленники.
4. Не вводите данные карты на чужих или общедоступных компьютерах (офис, интернет-кафе и т.п.), если вы не уверены в их безопасности.
5. Перед вводом реквизитов проверяйте строку адреса в браузере. Адрес должен начинаться с https://, а рядом отображаться значок замка. Через этот значок можно посмотреть информацию о сертификате сайта.
6. Сохраняйте в закладках адреса часто используемых интернет-магазинов и интернет-банка, чтобы не переходить по сомнительным ссылкам и не попасть на поддельный сайт с похожим именем.
7. Оформите отдельную карту для оплаты в интернете и подключите к ней онлайн-банк. Переводите на нее только сумму, необходимую для конкретной покупки, чтобы снизить возможные риски.
8. Если вы получаете ссылку для оплаты, лучше скопировать ее и вручную вставить в адресную строку браузера, чем переходить по клику из письма или мессенджера.
9. Подключите SMS- или push-уведомления по карте, чтобы оперативно видеть все списания и платежи.
10. Избегайте пересылки фотографий карты. Если это неизбежно, договоритесь с получателем о немедленном удалении фото после получения и удалите его у себя

(из почты, чата, облака). Конфиденциальные данные не отправляйте единым сообщением.

11. Перед подтверждением платежа обязательно проверяйте итоговую сумму и состав заказа. Магазин может по умолчанию добавить платные опции: дорогую доставку, страховку, дополнительные услуги.
12. Внимательно читайте условия «бесплатных» пробных периодов. Часто для доступа к сервису нужно ввести данные карты, а по окончании пробного периода начинается платная подписка, если ее заранее не отменить.
13. Регулярно проверяйте выписки и историю операций по карте. При обнаружении незнакомых списаний сразу обращайтесь в банк.