Ваши данные доступны только вам

Доступ к вашим данным имеете только вы и никто более. Никто из наших сотрудников, за исключением двух человек нашей компании, не имеет доступа к административной панели и серверам проекта. Мы не используем ваши данные в личных целях и не раскрываем их третьим лицам. Наш бизнес связан с реализацией удобного сервиса и никак не пересекается с деятельностью вашей компании.

Полное резервирование данных

Все ваши данные мы бережно охраняем и принимаем все необходимые меры для их сохранности. С периодичностью в несколько часов в автоматическом режиме
мы копируем все ваши данные и сохраняем их на защищенном внешнем носителе, что позволяет нам восстановить систему даже после полного выхода из строя серверов проекта.

Надежность работы системы

Для обеспечения надежности работы системы мы используем географически распределенную сеть серверов, расположенную в Российской Федерации. Данные между ними постоянно синхронизируются в режиме реального времени, что исключает потерю данных в случае нештатной ситуации. В случае какой-либо аварии, в кратчайшие сроки, все запросы будут переведены на доступный сервер.

Шифрование канала передачи данных

Все передаваемые данные между вашим браузером и серверами проекта защищены сертификатом безопасности SSL. 256-битный механизм шифрования предотвращает несанкционированный доступ к передаваемым пакетам между вашим компьютером и ПО для ЭВМ «WABABA».

Защита авторизации

Авторизовываясь в ПО для ЭВМ «WABABA», вы можете быть уверены,
что ваша сессия не будет похищена и использована для хищения ваших данных. Сессии пользователей хранятся в специальных таблицах БД, имеют ограниченный период жизни, идентификатор сессии меняется раз в несколько минут, что позволяет делать хищение сессий бесполезным для злоумышленников.

Правоохранительным органам

Мы готовы обеспечить всестороннее содействие правоохранительным органам, чтобы пресекать и расследовать преступления, связанные с кибермошенничеством.

Если возникнут подозрения или появятся факты, свидетельствующие об использовании сайта senseibpm.com в мошеннических целях, мы просим сотрудников правоохранительных органов связаться с нашей службой поддержки по электронному адресу info@wababa.ru или по телефону +79214329940.

Покупателям

Если вы пострадали от мошенничества при использовании сайта wababa.ru, пожалуйста, свяжитесь с нашей службой поддержки. Мы окажем всю необходимую помощь правоохранительными органами при проведении расследования и при пресечении дальнейших возможных противоправных действий с использованием ваших данных.
По всем вопросам, связанным с безопасностью, обращайтесь по электронному адресу info@wababa.ru или по телефону +79214329940 или направьте свое заявление по адресу: 127015, г. Москва, ул. Большая Новодмитровская, д. 36, стр.12, этаж 1, комната 9.

ООО «Витаргет» не берет на себя ответственность за расходы, понесенные в результате мошеннических действий со стороны третьих лиц. Помните — мы не принимаем оплату наличными. Если вам выставлен счет на оплату услуги, которую вы не заказывали, а также если у вас возникли сомнения в том, что вы имеете дело с представителем ООО «Витаргет» или с подлинными счетами нашей компании, свяжитесь с нами по электронной почте или по телефону. Пожалуйста, сообщайте нашей службе поддержки о любых подозрительных или явно мошеннических письмах, ссылающихся на услуги ООО «Витаргет».

Советы по безопасности

Используйте для покупок через интернет отдельную банковскую карту, на который вы не храните постоянные средства. Пополняйте карту на необходимую сумму непосредственно перед совершением покупок и используйте ее только для онлайн-шопинга.
Никогда и никому не передавайте свою банковскую карту. Злоумышленнику достаточно сфотографировать обе стороны вашей карты, чтобы он смог использовать ваш счет для совершения собственных покупок.
Чтобы злоумышленник не мог воспользоваться вашей картой для покупок в интернете, заклейте трехзначный проверочный CVC-код на тыльной стороне карты: тогда его невозможно будет прочесть. Например, код можно замаскировать специальной замазкой ленточного типа для бумаги — это абсолютно безопасно для карты.
Если ваша карта находится при вас, но вы получили SMS-сообщение о совершении платежной операции с ее использованием, незамедлительно произведите оплату этой картой в любой ближайшей торговой точке. Совершенно неважно, что в этой ситуации
покупать (это может быть любая мелочь), — важно, что даже при отсутствии средств попытка транзакции будет зафиксирована системой. Поскольку для мошеннических операций используются украденные реквизиты карты или ее созданный дубликат, то при помощи этого простого действия вам будет проще доказать, что вы отсутствовали на месте проведения мошеннической транзакции. А географическое положение мошенников будет установлено по IP-адресу компьютера, с которого осуществлялся платеж, или номеру терминала, где ими были получены наличные.
Имейте в виду, что банк никогда не переводит деньги продавцу сразу в момент покупки. Запрошенная торговой точкой сумма сначала резервируется и лишь спустя сутки или даже несколько поступает на счет продавцу. За это время можно успеть опротестовать и заблокировать любую транзакцию, обратившись в банк с соответствующим заявлением.

Не смущайтесь, если банк выдал вам карту, не требующую ввода ПИН-кода при покупках в торговых сетях. Такой принцип оплаты относится к более безопасным, чем тот, к которому вы привыкли. Отсутствие необходимости подтверждения ПИН-кодом сохраняет эти четыре секретные цифры от посторонних глаз, ведь вам их не нужно вводить при оплате. Оспорить транзакцию, совершенную с вводом ПИН-кода, который согласно договору с банком должен быть известен только вам, практически невозможно, а вот деньги, списанные с карты без ввода ПИН-кода на терминале, можно вернуть.

Подключите услугу SMS-информирования обо всех финансовых операциях с вашей платежной картой. При получении сообщения о несанкционированной транзакции немедленно обратитесь по телефону в свой банк.