РЕКОМЕНДАЦИИ АО «БАНК ОРЕНБУРГ» ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ РАБОТЕ С БАНКОВСКИМИ КАРТАМИ

Уважаемые клиенты! Предлагаем вам внимательно ознакомиться с материалами раздела, перед тем как совершать какие-либо операции с банковской картой. Помните, что ваша финансовая безопасность зависит в том числе и от вашего ответственного отношения к собственным персональным данным при использовании карт.

С каждым годом увеличивается объем несанкционированных операций с использованием платежных карт посредством сети «Интернет» и мобильных устройств. Способы весьма разнообразны.

ИСПОЛЬЗОВАНИЕ ПОДДЕЛЬНЫХ САЙТОВ (ФИШИНГ)

Схема обмана такова: злоумышленники размещают в поисковых системах ссылки на сайты с выгодными предложениями о покупке различных товаров и услуг. Дизайн этих страниц ничем не отличается от оформления настоящих интернет-магазинов. Операции на таких сайтах, замаскированные под оплату товаров и услуг, на деле представляют собой перевод денежных средств на счета мошенников. После завершения такой "оплаты" вы даже можете получить по электронной почте уведомление, подтверждающее факт заказа или бронирования, но реальный товар или услугу вы никогда не получите. При этом следует помнить о том, что денежный перевод (на электронный кошелек или на карту) является безотзывным и не может быть впоследствии оспорен.

Чтобы не стать жертвой мошенников, необходимо следовать нескольким простым правилам.

- Приобретайте дорогостоящие товары (телефоны, компьютерную технику и пр.) с доставкой только на известных интернет-площадках.
- Распознать обман можно по ценам, привлекательно отличающимся от средних цен на аналогичные предложения других продавцов. До совершения покупки следует ознакомиться с отзывами о сайте, на котором размещено выгодное предложение.
- Также можно проверить подозрительный сайт на специализированных сервисах. Если сайт зарегистрирован на физическое лицо или сайту не больше месяца - более чем вероятно, что сайт – мошеннический.

Уважаемые клиенты! Так как в условиях стремительно развивающихся современных технологий количество совершаемых сделок в интернете с каждым годом увеличивается, АО «БАНК ОРЕНБУРГ» настоятельно рекомендует Вам придерживаться вышеизложенных правил при работе с

интернет-ресурсами, чтобы радость от покупки новой вещи не превратилась в разочарование от потери денежных средств.

МОШЕННИЧЕСТВО С ПОМОЩЬЮ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Именно мошенничество, связанное с обманом держателя карты, является в настоящее время самым серьезным вызовом безопасности использования банковской карты. Обезопасить себя от угроз, сопряжённых с манипулированием и обманом можно соблюдая простые меры безопасности, изложенные как на нашем сайте, так и в разнообразных раздаточных материалах на бумажных носителях.

Обман при продаже товаров на интернет-аукционах

Злоумышленники используют два чрезвычайно распространенных способа обмана и кражи средств при осуществлении сделок на интернет-аукционах.

1. Добросовестный продавец размещает информацию о продаже некоего товара на общедоступной аукционной площадке. Мошенники под видом покупателей связываются с продавцом и просят предоставить им реквизиты карты для осуществления предоплаты. Используя полученную информацию (часто держатели карт разглашают не только номер карты, но и CVC2-код, а также одноразовые пароли 3D Secure), злоумышленники переводят деньги с карты жертвы на свои карты (телефонные счета и пр.).
2. Добросовестный покупатель обращается к продавцу (мошенникам под видом продавца) в целях приобретения того или иного товара, после чего мошенники просят произвести предоплату путем перевода средств с карты на карту или электронный кошелек. Получив деньги, продавец перестает выходить на связь.

Фальшивые SMS-рассылки

По случайным номерам осуществляется рассылка SMS-сообщений о блокировке карты с указанием номера телефона для получения дополнительной информации. При звонке на указанный номер мошенники, представляющиеся работниками Службы безопасности, сообщают о необходимости произвести те или иные действия с картой, результатом которых становится перечисление средств клиента на счета и мобильные телефоны мошенников. АО «БАНК ОРЕНБУРГ» настоятельно рекомендует своим клиентам не перезванивать на любые телефонные номера, не совпадающие с указанными на сайте банка, а также никому не раскрывать конфиденциальную информацию о вас или вашей банковской карте. Не

предоставляйте никакой информации, даже если вам представились сотрудником банка.

Звонок от «Сотрудника Банка»

Злоумышленник, представившись сотрудником банка, в ходе телефонного звонка сообщает держателю карты, что база данных банка по какой-либо причине пострадала и для ее восстановления необходимо сообщить номер карты, PIN-код, срок её действия, защитный код CVC2. При этом он может правильно назвать ваше имя, фамилию и даже кодовое слово. Но, несмотря ни на что, никогда и никому не сообщайте выше указанные данные, так как эта информация является первоосновной защитой ваших финансов.

Сектор «Приз»

Речь идёт о давно известных, но продолжающих работать поддельных розыгрышах ценных призов от имени известных компаний. Злоумышленники предлагают оплатить с помощью электронных денег «налог на выигрыш» или стоимость пересылки приза. Пользователям необходимо проверять информацию о подобных выигрышах, обращаясь за подтверждением к предполагаемому организатору.

Взлом персональных страниц в социальных сетях

Злоумышленники взламывают персональную страничку пользователя на популярном социальном интернет-ресурсе (в социальных сетях, мессенджерах), после чего производят рассылку сообщений по всему списку контактов с просьбой от имени владельца странички занять ему некоторую сумму. В процессе переписки с мошенниками знакомые пострадавшего лица часто соглашаются одолжить деньги, которые злоумышленники практически всегда просят перевести на указанные ими электронный кошелек или карту. Будьте бдительны в подобных ситуациях и всегда проверяйте информацию, пользуясь альтернативными каналами связи.

Звонок «близкого человека»

Злоумышленник звонит вам от лица родственника или близкого человека с просьбой о помощи. Как правило, описывается какая-либо угрожающая ситуация (вплоть до привлечения к уголовной ответственности), из которой можно помочь выйти, передав определенную сумму денег нужному лицу. Зачастую, находясь в состоянии психологического напряжения, человек, не задумываясь, отдает мошенникам наличные деньги либо совершает перевод по указанным ими реквизитам. Будьте бдительны в

подобных ситуациях и всегда проверяйте информацию, пользуясь альтернативными каналами связи.

Важно отметить, что по всем вышеизложенным схемам отозвать или оспорить мошеннический перевод банки не имеют возможности, и держателю карты необходимо обращаться в правоохранительные органы.

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Распространение вирусов для мобильных устройств позволяет злоумышленникам незаметно получать и использовать данные банковских карт, кодов подтверждения и паролей для проведения операций в системе «Интернет-банк» АО «БАНК ОРЕНБУРГ».

Чтобы не стать жертвой мошенников, устанавливайте и своевременно обновляйте на мобильных устройствах антивирусные программы от ведущих производителей. Скачивайте и устанавливайте программы (приложения) только из официальных источников. Никогда не сообщайте позвонившим лицам реквизиты своей банковской карты, не разглашайте пароли и коды подтверждения, выданные Вам в рамках подключенных банковских услуг (сервисов). Не предоставляйте никакой информации, даже если вам представились сотрудником банка.

НЕДОБРОСОВЕСТНЫЕ ФОРЕКС-ДИЛЕРЫ, ФИНАНСОВЫЕ ПИРАМИДЫ

Мы предупреждаем своих клиентов о потенциальной опасности вложения денежных средств в различные интернет-компании, которые зачастую позиционируют себя как форекс-дилеры, предлагающие разного рода высокодоходные инвестиционные инструменты (доверительное управления финансами на внебиржевом рынке Forex, торговля «бинарными опционами» и т.д.). В условиях нестабильности на финансовых рынках значительная часть подобных организаций, изначально организованных по принципам «финансовых пирамид» или интернет-казино, самоликвидировались, не исполнив обязательств перед вкладчиками.

Особенную осторожность следует проявлять в случаях:

- обещания различных эксклюзивных предложений с гарантированной высокой доходностью;
- отсутствия полных реквизитов организации, её банковских счетов;
- оффшорной юрисдикции компании (головного офиса);
- отсутствия возможности личного визита в офис компании для заключения договора и ознакомления с правоустанавливающей документацией.

Необходимо отметить, что процедура вложения средств в недобросовестные инвестиционные компании организована таким образом, что принудительный возврат инвестиций практически невозможен: переводы являются безотзывными с точки зрения как действующего законодательства РФ, так и международных платежных систем (в случае перевода средств с помощью банковских карт).

ПРОТИВОПРАВНЫЙ ДОСТУП ЗЛОУМЫШЛЕННИКОВ К SIM-КАРТАМ ДЕРЖАТЕЛЕЙ БАНКОВСКИХ КАРТ

Существует риск хищения средств с банковских карт, связанный с противоправным доступом злоумышленников к SIM-картам держателей банковских карт.

Настоятельно рекомендуем:

1. контролировать активность (рабочее состояние, доступ к сети и услугам связи) SIM-карты, номер которой подключен к каким-либо сервисам АО «БАНК ОРЕНБУРГ»;
2. при нехарактерном пропадании связи на мобильном устройстве с SIM-картой незамедлительно связаться с оператором сотовой связи и принять меры к временной блокировке карты одним из доступных способов.

Дополнительно напоминаем о необходимости своевременно информировать банк об обновлении/изменении данных (в т.ч. номера мобильного телефона).

АО «БАНК ОРЕНБУРГ» РЕКОМЕНДУЕТ СВОИМ КЛИЕНТАМ ПОДКЛЮЧИТЬ СЕРВИС «SMS-ИНФОРМИРОВАНИЕ», ТАК КАК ОН СОДЕРЖИТ В СЕБЕ УСЛУГУ SECURE CODE

Технология 3-D Secure является современным стандартом обеспечения безопасности платежей при проведении расчетов по банковским картам в интернете. На базе технологии 3-D Secure международными платежными системами разработаны специальные программы - Verified by Visa и MasterCard® SecureCode™. В рамках этих программ при совершении платежа в интернете держатель карты после ввода реквизитов карты автоматически перенаправляется на специальную защищенную страницу интернет-сайта АО «БАНК ОРЕНБУРГ», где он подтверждает проведение платежа путем ввода одноразового пароля.

Обращаем Ваше внимание, что не все интернет-магазины поддерживают технологию 3-D Secure. Как правило, признаком использования технологии 3-D Secure является размещение на сайте магазина логотипов программ Verified by Visa и/или MasterCard® SecureCode™.

Уважаемые клиенты! Если вы обнаружили пропажу карты или у вас есть основания полагать, что данные карты могут быть использованы третьими лицами, или вы получили сообщение об операции (или попытке операции), которую не совершали – незамедлительно проинформируйте об этом АО «БАНК ОРЕНБУРГ» и заблокируйте карту.

Вы можете это сделать, позвонив по одному из нижеуказанных телефонов или обратившись в любой из наших офисов:

+7 (3532) 343-103
+7 (3532) 205-552
+7 (383) 363-1158
+7 (495) 924-7500

+7 (800) 200-4575 (Звонок по России бесплатный)

- офисы в Оренбурге
- офисы в Оренбургской области