**Дистанционное мошенничество**.

Сегодняшнее повествование пойдет о важнейшей проблеме, с которой сталкивались многие граждане – это дистанционное мошенничество, в том числе интернет-мошенничества и получение мошенниками удаленного доступа к банковской карте.

В рамках повествования необходимо рассказать об ответственности за деяния в данной сфере, виды мошеннических действий, признаки мошенников, меры предупреждения таких преступлений.

Ответственность за использование чужого доверия с целью завладения средствами, привязанными к платежной карте, предусматривается в ст. 159.3 Уголовного кодекса Российской Федерации.

Согласно ч. 1 ст. 159.6 УК РФ под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

За данное преступление предусмотрена ответственность в виде штрафа в размере до 120 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо арест на срок до четырех месяцев.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. ст. 272, 273 или 274.1 УК РФ.

Согласно ч. 1 ст. 159.3 УК под мошенничеством с использованием платежных карт понимается хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Это деяние наказывается штрафом в размере до 120 рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

Данной статьей предусмотрены также отдельные классифицирующие признаки.

С конца 2018 года по статьям 159.3 и 159.6 УК снижено пороговое значение крупного размера с 1,5 млн рублей до 250 тыс. рублей, особо крупного - с 6 млн рублей до 1 млн рублей.

Далее рассмотрим наиболее распространенные способы незаконного овладения чужими средствами или данными, являющимися собственностью правообладателя.

Одним из самых распространенных видов интернет-мошенничества является так называемый «Фишинг».Мошенники совершают определенные действия, направленные на получение доступа к денежным средствам на банковской карте потенциальной жертвы, при помощи почтовых рассылок от лица банка, содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов, на которых предлагается ввести данные карты для возможности дальнейшего ее использования.

Еще одним крайне распространенным видом интернет-мошенничества являются фальшивые интернет-магазины. Мошенники берут с покупателя предоплату за товар и не выполняют своих обязательств.

Важно отметить, что популярность в поисковике вовсе не гарантия вашей безопасности. На самом деле мошенники активно продвигают свои сайты с использованием вебмаркетинга. И зачастую фальшифкистоят даже выше ссылок на оригинальный сайт и внешне он на первый взгляд ничем не отличается от оригинала. Платежные страницы на таких сайтах только маскируются под оплату товаров и услуг, на самом деле потенциальная жертва переводит деньги на карты мошенников или на номера мобильных телефонов, с которых впоследствии мошенники снимут деньги. Кроме того на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций. После совершения такой оплаты, жертва даже может получить подтверждение по почте, но товаров ни услугдоставлено и оказано не будет.

**Как же отличить поддельные сайты от настоящих?**

Первое – внимательно изучите адресную строку. Дизайн может полностью копировать оригинальный сайт, но в адресной строке точно будет что-то не так, хотя бы один символ.

Второе – сайт новый и о нем нет никакой информации в интернете.

Третье – тексты на сайте могут содержать ошибки и неработающие ссылки.

Четвертое – дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка, а еще название магазина будет написано порски, а не латинскими буквами как обычно в легальных платежных системах.

Пятое – вместо названия магазина на аутентификационной странице символы Р2Р, PEREVODNAKARTU, или CARD2CARD, то есть информация о переводе средств с карты на карту.

Шестое – сумма на аутентификационной странице банка может быть изменена.

Седьмое – после введения корректных данных сайта для одноразового пароля жертве сообщают, что пароль неверный и просят ввести новый пароль на самом деле, чтобы провести новую операцию.

Заметив любой из этих признаков, звоните по телефону, который указан на вашей карте и пользуйтесь только проверенными интернет-площадками.

Крайне распространенным способом мошенничества является мошенничество в социальных сетях. Мошенники взламывают персональную страницу пользователя в социальных сетях или мессенджере и либо всем подряд отправляют сообщения с просьбой помочь и срочно перевести денег, либо анализируют переписку и находят самых близких людей, тех, кто точно не откажет.

После первого перевода мошенники могут связаться с жертвой, сказать, что-то пошло не так, попросить повторить перевод и так пока на карте не закончатся деньги или жертва не догадается об обмане, но выманивать могут не только деньги, но и реквизиты карт якобы для того, чтобы перевести деньги жертве, спросят номер карты, срок действия, трехзначный код безопасности и пароли из смс, однако деньги жертве разумеется не придут, зато с карты средства будут списаны.

Что же делать, если вам пришло сообщение с просьбой о помощи от одного из знакомых или родственников? Необходимо немедленно связаться с ним по телефону, уточнить отправлял ли он это сообщение и не предпринимать ничего, пока он не подтвердит это лично. Тем более ни в коем случае нельзя сообщать реквизиты своей карты (три цифры на оборотной стороне, срок действия, пароль из смс, кроме того нужно позаботиться и о пароле для своего аккаунта в соцсетях и мессенджерах. Он защищает не только вашу безопасность, но и безопасность ваших родных и близких.

Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов» или «подключения к социальной программе» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

Важно помнить, что при звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты карты и совершать какие-либо операции с картой.

Если вам позвонили из банка, и интересуются вашей платежной картой, разумнее всего прекратить разговор и перезвонить в банк по официальному номеру контактного центра банка (номер телефона службы поддержки клиента указывается на оборотной стороне карты).

Более подробно остановимся на данных, которые могут быть запрошены у жертвы мошенниками.

ПИН-код карты – четырехзначная комбинация цифр, выдаваемая в конверте одновременно с изготовленной банковской картой. Его можно изменить, обратившись в отделение банка или позвонив на горячую линию.

Код безопасности (CVV2 или CVC2) – комбинация цифр, указанная на оборотной стороне карты, а именно: три крайние правые цифры, указанные после четырех последних цифр номера карты. Проверочный код необходим

только для совершения платежей в интернете. При онлайн-оплате он вводится вместе с номером карты, именем держателя карты и сроком окончания действия карты.

Одноразовый пароль банка для подтверждения оплаты онлайн – комбинация цифр, отправляемых банком в смс-сообщении или push- уведомлении для подтверждения операций с денежными средствами.

Ни в коем случае не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам!

Никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить ПИН-код или код безопасности. А одноразовый пароль вводится при совершении онлайн-покупки на странице с защищенным соединением.

Кодовое слово держателя карты – информация, указанная клиентом банка при оформлении карты. Кодовое слово необходимо для идентификации клиента при звонке в контакт-центр банка. Рекомендуется использовать кодовые слова, которые злоумышленникам будет очень сложно узнать. Подумайте о том, что случилось с Вами в детстве или юности, вспомните место действия, объект, человека или событие – пусть оно будет Вашим кодовым словом.

Код клиента банка – комбинация цифр, используемая для сокращения времени на идентификацию клиента при обращении в контакт-центр.

Сообщать кодовое слово или код клиента банка можно только в том случае, если вы обратились в контакт-центр и разговариваете с сотрудником банка.

Подробнее остановимся на том, как безопасно пользоваться интернет-банком.

Используйте сложный пароль блокировки экрана и качественную антивирусную программу. Не входите в банковские приложения, используя отпечаток пальца или функцию распознавания лица.

Ни в коем случае не храните в телефоне логин и пароль от входа в мобильный банкинг.

Не храните в телефоне реквизиты карты: номер, срок действия, проверочный код и ПИН-код карты.

Избегайте входа в систему мобильного банкинга с чужих устройств.

При утрате телефона немедленно обратитесь в банк для блокировки карты и в офис мобильного оператора для блокировки SIM-карты.

Не переходите по ссылкам из SMS-сообщений, даже если в сообщении утверждается, что оно из банка.

Отключите функцию отображения текста входящих SMS- уведомлений на экране заблокированного телефона.

**Как безопасно совершать платежи в интернете?**

Используйте на устройстве антивирус с активной защитой онлайн- платежей.

Совершайте оплату только посредством использования защищенных соединений. Защищенное или зашифрованное подключение можно распознать по значку в виде замочка в начале адресной строки браузера и префиксу https:// (не просто http, а с буквой s на конце) перед адресом сайта.

Всегда завершайте сеанс в интернет-банке перед тем, как закроете вкладкубраузера.

Не проводите финансовые операции с общественного WI-FI в кафе, транспорте или гостиницах.

Не сохраняйте свои данные о карте в браузере.

Если все-таки мошенникам удалось совершить преступление, то жертве необходимо обратиться в полицию с заявлением, сохранить ссылки на сайты, с которых были совершены мошеннические действия, переписку с мошенниками и другие данные, которые могут быть полезны для идентификации мошенник.