Дистанционное мошенничество

Важнейшей проблемой, с которой сталкивались многие граждане – это дистанционное мошенничество, в том числе интернет-мошенничества и получение мошенниками удаленного доступа к банковской карте.

Самыми распространенными видами интернет-мошенничества является:

- так называемый «Фишинг», это когда 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.

- 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 веб-маркетинга. И зачастую фальшивки стоЯт 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.

- 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.

Как же отличить поддельные сайты от настоящих?

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

2. сайт новый и о нем нет никакой информации в интернете.

3. тексты на сайте могут содержать ошибки и неработающие ссылки.

4. 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.

5. вместо названия магазина на странице сайта имеются символы P2P, PEREVODNAKARTU, или CARD2CARD, то есть информация о переводе средств с карты на карту.

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

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 соц-сетях 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.

ПОМНИТЕ! 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).

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.

Как безопасно пользоваться интернет-банком.

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

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

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

4. Избегайте входа в систему мобильного банкинга с чужих устройств.

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

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

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

Как безопасно совершать платежи в интернете?

1. Используйте на устройстве антивирус с активной защитой онлайн- платежей.

2. 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.

3. Всегда завершайте сеанс в интернет-банке перед тем, как закроете вкладку браузера. Не проводите финансовые операции с общественного WI-FI в кафе,

транспорте или гостиницах.

4. Не сохраняйте свои данные о карте в браузере.

Если все-таки мошенникам удалось совершить преступление, то жертве необходимо обратиться в полицию с заявлением или по телефону 112, сохранить ссылки на сайты, с которых были совершены мошеннические действия, переписку с мошенниками и другие данные, которые могут быть полезны для идентификации мошенник

Ответственность.

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.

Пример:

На территории г. Кольчугино в 2021 году совершено такое преступление.

Так, у 30-летнего местного жителя возник преступный умысел на хищение денежных средств гражданина путем размещения в одной из социальных сетей информации о наличии у преступника предметов со спортивной символикой, тогда как в действительности их не было.

На данное предложение откликнулся потерпевший, проживающий в г. Волгоград и в период со 02.11.2021 по 10.11.2021 через переписку в социальной сети, злоумышленник путем обмана и злоупотребления доверием сообщал потерпевшему о наличии у него различных предметов со спортивной символикой – мягкие игрушки, значки, шарфы, кружки в подтверждение чего отправляя потерпевшему взятые из интернета изображения. Потерпевший в свою очередь, будучи не осведомленным о преступных намерениях злоумышленника переводил денежные средства со своего банковского счета на банковский счет злоумышленника. Всего таким способом было похищено 59 100 рублей, что причинило значительный ущерб потерпевшему.

Таким образом, совершено преступление, предусмотренное ч. 2 ст. 159 УК РФ мошенничество, то есть хищение чужого имущества путем обмана, совершенное с причинением значительного ущерба гражданину.

В ходе предварительного следствия обвиняемый в содеянном раскаялся, вину в совершенном преступлении признал полностью.

Уголовное дело рассмотрено Кольчугинским городским судом, за совершенное преступление, назначено наказание в виде обязательных работ на срок 300 часов.