Мошенничества, совершаемые с использованием информационно-коммуникационных технологий

В настоящее время факты мошенничества в различных сферах жизни стали распространенным явлением. Многие преступники поняли, что для получения незаконного обогащения надежнее действовать не силой, а хитростью. Мошенничество как вид преступности опасен не меньше, чем грабежи и разбои. Потерпевший в силу субъективных и объективных причин безоружен перед мошенниками, которые в отличии от грабителей обезоруживают потерпевшего не физически, а морально, совершая преступления с использованием современных информационно-коммуникационных технологий. Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «на вас пытаются оформить кредит или похитить деньги», «сбой в базе данных», «начисления бонусов», «подключения к социальной программе» или «иных надуманных предлогов» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета.

Так 09февраля 2022 года в УМВД России по городу Чите обратилась женщина и сообщила о хищении 400 тысяч рублей с банковской карты. Сотрудники полиции установили, что у женщины перестала работать услуга «Мобильный банк». Для решения вопроса она обратилась в техническую поддержку банка. Через некоторое время ей позвонили и попросили назвать персональные данные, а также реквизиты банковской карты. Женщина, будучи уверена, что звонит сотрудник банка по оставленной ею заявке, продиктовала все данные, после чего с двух карт разных банков были похищены денежные средства. По факту хищения денежных средств возбуждено уголовное дело, сотрудниками полиции устанавливаются обстоятельства произошедшего, а также лица, совершившие хищение.

Злоумышленники заставили забайкалку купить смартфон, подключить услугу «Google Pay», добавить 12 банковских карт и перевести на них деньги. В отдел полиции обратилась 60-летняя местная жительница и сообщила о хищении крупной суммы денег. Полицейские установили, что женщине позвонил неизвестный и, представившись сотрудником службы безопасности банка, клиентом которого является потерпевшая, спросил, делала ли она заявку на снятие денег со сберегательного счета и оформление кредита. Получив отрицательный ответ, злоумышленник предупредил, что это могут действовать возможные мошенники и рекомендовал срочно обналичить деньги. Читинка пошла в банк и сняла со счета 1 900 000 рублей Все это время позвонивший мужчина находился на связи с потерпевшей, требовал ни с кем не общаться, не объяснять работникам банка причины снятия денег Затем, выполняя указания злоумышленника, читинка пошла в магазин и приобрела мобильный телефон, подключив на него услугу бесконтактной оплаты. Когда женщина пришла домой, мошенник дистанционно научил женщину, как добавить в «Google Pay» банковские карты, диктуя их номера. Выполняя указания, потерпевшая добавила 12 чужих банковских карт, и на следующий день через банкомат с помощью подключённой услуги на телефоне, перевела обналиченные 1 900 000 рублей на карты. Затем в течение нескольких дней ей звонили и просили оформить кредиты, а деньги для сохранности перевести на добавленные ранее банковские карты. Доверчивая забайкалка оформила четыре кредита в разных банках на общую сумму девять с половиной миллионов рублей и перевела их мошенникам. Девять дней мошенники держали забайкалку «на крючке», часами не позволяя отключаться от телефонного разговора, сопровождая каждый ее шаг. За это время ей звонили с 30 номеров телефонов, в том числе, представляясь сотрудниками полиции из Москвы и Читы, убеждая не останавливаться и продолжать брать кредиты, чтобы помочь следствию задержать мошенников, действующих в банковской сфере. Мошенники могут представляться кем угодно, в том числе сотрудниками правоохранительных органов и использовать сервисы, позволяющие осуществить подмену номера телефона. В таком случае на телефоне потерпевших «высветится» номер с кодом города Читы, в том числе номера телефонов отделов полиции и других структур. Категорически запрещено вступать в разговоры с неизвестными, особенно когда речь идет о банковских операциях, тем более осуществлять переводы денег или оформлять кредиты по указаниям звонивших. Никаких «безопасных счетов» или «безопасных ячеек» не существует - это номера сотовых телефонов с привязанными к ним банковскими счетами и картами, принадлежащих мошенникам.

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.

Интернет-Покупки

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 сайта в поисковике вовсе не гарантия вашей безопасности. В действительности мошенники активно продвигают свом сайты с использованием вебмаркетинга. 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. Кроме того, на поддельных сайтах мошенники собирают реквизиты карт, которые потом используют для несанкционированных операций. После совершения такой оплаты покупатель даже может получить подтверждение по почте, но товаров и услуг доставлено и оказано не будет.

Признаки отличия поддельных сайтов от настоящих:

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

- Сайт новый и о нем нет никакой информации в интернете.

- Тексты на сайте могут содержать ошибки и неработающие ссылки.

- Дизайн страницы ввода одноразового пароля может отличаться от привычного дизайна вашего банка.

- Вместо названия магазина на аутентификационной странице символы P2P, PEREVODNAKARTU или CARD2CARD, то есть информация о переводе средств с карты на карту.

- Сумма на аутентификационной странице банка может быть изменена.

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.

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.

Оказание интимных услуг:

Так, например, житель областного центра в Сети нашел сайт с предложениями интимных услуг. Выбрав понравившуюся девушку, он позвонил по указанным контактам и договорился о встрече, собеседница попросила перечислить предоплату. Потерпевший выполнил ее просьбу, воспользовавшись терминалом. Пока потерпевший ждал приезда девушки, она позвонила и сообщила о необходимости доплатить - по указанным реквизитам он перевел требуемую сумму. Позже позвонил уже мужчина: по его словам, переводы не прошли, поэтому их нужно повторить. Читинец выполнил и это требование. Но новая знакомая так и не приехала. После этого ему позвонил мужчина, который сообщил, что по вине мужчины у них зависла касса и

необходимо еще дополнительно перевести денежные средства. Переведя в общей сложности около 13 тысяч рублей и так и не дождавшись ни девушки, ни возврата денег, мужчина обратился в полицию. Также при отказе от уже заказанных услуг девушек, могут звонить мужчины, угрожать применением физической расправы или распространением информации родственникам.

Инвестиции

Пример: Забайкалец в сети Интернет увидел рекламу инвестирования в популярную бизнес-компанию и, перейдя по ссылке, оставил свои контактные данные. Через некоторое время ему позвонил мужчина, который представился координатором брокерской площадки и рассказал возможности получения дохода путем покупки акции газовой компании. Потерпевшему предложили скачать специальное приложение и программу для отслеживания своего инвестиционного счёта. Около четырех месяцев мужчина якобы зарабатывал на данной платформе, периодически внося деньги на счет. За это время забайкалец оформил два кредита на общую сумму более 1 500 000 рублей. Решив вывести с площадки свои деньги и якобы полученный доход, у потерпевшего потребовали оплату страховки и других услуги, а также сообщили, что его счет заблокирован. Забайкалец понял, что стал жертвой мошенников и обратился в полицию.

Злоумышленники могут использовать самые разные способы обмана, чтобы похитить деньги. Самое главное правило - это не вступать в телефонные разговоры с неизвестными, кем бы они не представлялись, и ни под какими предлогами не совершать операции по переводу и обналичиванию денежных средств.

21 Ноября 2022

Адрес страницы: https://zabaykalye.sledcom.ru/Ostorozhno-moshenniki-/item/1742004