Приложение

К наиболее частым мошенническим действиям относятся следующие способы:

1**. Преступления, совершенные под предлогом попытки списания денежных средств с банковской карты.**

На абонентский номер потерпевшего поступает телефонный звонок, в ходе которого звонящий представляется сотрудником безопасности какого-либо финансово-кредитного учреждения и сообщает потерпевшему, что на его имя оформлен или пытаются оформить кредит мошенники и для защиты денежных средств необходимо осуществить снятие денежных средств с банковского счета и зачислить их на «безопасный счет», который сообщается злоумышленником. По легенде это временная мера – на период поиска преступников. А потом всю сумму человеку якобы возместят наличными в приемной Банка России в Москве.

В данном случае необходимо знать, что:

- сотрудники полиции, ФСБ, банков никогда не звонят по вопросам сохранности сбережений;

- не существует «безопасного счета», на которые требуют перевести денежные средства;

- сотрудники полиции никогда не привлекают граждан для выявлении недобросовестного сотрудника банка;

- сотрудники полиции, ФСБ, банков никогда не звонят гражданам посредством мессенджеров;

- сотрудник банка не требует сообщить номер банковской карты, трехзначный код на оборотной стороне карты, кодовое слово, пароли и коды доступа к личному кабинету онлайн-банка;

- поступивший код в смс-сообщении запрещается сообщать кому-бы то ни было;

- сотрудники полиции, ФСБ, банков не сообщают, что от имени потерпевшего подана заявка на продажу квартиры и для предотвращения сделки купли-продажи необходимо самому подать заявку на продажу квартиры, а денежные средства перевести на «безопасный счет»;

- сотрудники полиции, ФСБ, банков никогда не предлагают воспользоваться услугой поддержки и установить на телефон приложения удаленного доступа, данное приложение позволяет не только видеть демонстрацию экрана потерпевшего, вводимые им пароли от онлайн-банка, но и самому выполнять активные действия с телефоном.

2. Преступления совершены под предлогом продления договора сим-карты с оператором сотовой связи.

Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту пользователя «Госуслуги».

Они звонят жертве и утверждают, что действующий договор заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет

злоумышленник. Достаточно продиктовать код из смс. Следующий шаг – перейти по ссылке, где нужно ввести еще один код. Таким образом человек предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая хранится на этом ресурсе.

В данном случае необходимо знать, что:

- договор оказания услуг связи является бессрочным и его не нужно продлевать;

- Вы можете обновить персональные данные, обратившись за услугой лично – в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из смс).

- не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору связи по номеру, который размещен на его официальном сайте.

3. Преступления совершены под предлогом оказания помощи родственнику, попавшему в полицию, в частности, как виновному в совершении ДТП.

Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, о том, что задержан сотрудниками полиции за совершение того или иного преступления (ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и др.). Далее в разговор вступает, якобы, сотрудник полиции, который поясняет, что для освобождения от уголовной ответственности необходимо передать денежные средства. Деньги необходимо привезти в определенное место, передать какому-либо человеку или перевести на определенный счет. Общественная опасность подобных преступлений заключается в том, что помимо причинения материального ущерба потерпевшим, дискредитируются правоохранительные органы;

В данном случае необходимо знать, что:

- при поступлении подобного звонка необходимо прервать разговор и перезвонить своему родственнику;

- запрещается передавать денежные средства лицам, которые пришли от имени сотрудников полиции.

4. Преступления совершены под предлогом дистанционной купли-продажи товаров посредством сети Интернет.

На интернет-сайтах по продаже товаров и услуг мошенниками выставляется объявление о продаже товара или предоставлении услуги. Потерпевший, заинтересовавшись предложением, связывается с продавцом-мошенником и переводит деньги на указанные последним счета банковских карт, электронные кошельки и счета абонентов операторов сотовой связи, но товар или услугу не получает и контакт с ним прекращается.

При продаже потерпевшими товаров или услуг, мошенники под предлогом перевода денег в виде предоплаты за покупку, путем обмана получают от последних информацию о банковских картах и паролях к ним или к системе «Мобильный банк», личным кабинетам пользователей услугами

банков «онлайн» и с помощью полученной информации похищают деньги потерпевших.

Также злоумышленники отправляют сообщение потерпевшим с предложением приобрести или продать товар, в дальнейшем преступник отправляет в сообщении ссылку по которой необходимо перейти для получения денежных средств за продаваемый товар или оплаты приобретаемого (проведение безопасной сделки, осуществления доставки). Перейдя по ссылке потерпевший попадает сайт (зеркало), схожий внешне с объявлением, где требуется ввести реквизиты банковской карты и код для подтверждения операции, в последующем со счета потерпевшего списываются денежные средства. В большинстве случаев, для совершения указанного вида преступлений злоумышленники используют приложения Телеграм с помощью которого генерируют ссылки, а также приобретают абонентские номера и аккаунты социальных сетей и таких сайтов как Авито, Юла и т.д.

В данном случае необходимо знать, что:

- при общении с продавцом, не следует переходить в другие мессенджеры для продолжения диалога и не переходить по ссылкам, которые он отправляет;

- при продаже товара потерпевшими, покупатель никогда не спрашивает дату выдачи банковской карты, трехзначный код на оборотной стороне карты, а так же поступившие в смс-сообщении пароли;

- при покупке дорогостоящего товара необходимо убедиться в надежности продавца, проверив активность его аккаунта;

- при покупке в Интернет магазинах внимательно читать название сайта в адресной строке, чтобы избежать сайта дублера, так как злоумышленник часто меняет один символ, который менее заметен.

5. Преступления совершены под предлогом инвестирования денежных средств в различные «финансовые пирамиды».

Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое – нужно лишь открыть «брокерский» счет и инвестировать от 10 000 рублей. Доход – не меньше миллиона. Для открытия такого счета мошенники требуют установить приложение. Далее программа имитирует якобы рост доходов от инвестиций, в том числе в криптовалюту. Как только у «инвестора» возникает желание вывести деньги со счета – начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства. В итоге инвестор теряет свои денежные средства.

В данном случае необходимо знать, что:

- не рекомендуется переходить по всплывающим окнам (банерам) в сети Интернет с рекламой инвестиций и заполнять анкеты с указанием своих персональных данных;

- проверьте сайт инвестиционной компании или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России;

- откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица (либо через электронный кошелек);

- обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.

- не ведитесь на обещания гарантированного высокого дохода в короткие сроки;

6. Преступления совершены под предлогом займа денежных средств от знакомых.

Злоумышленник взламывает аккаунт пользователя социальной сети (Одноклассники, Вконтакте) и рассылает сообщение с просьбой одолжить денег близким или друзьям.

С развитием современных технологий злоумышленники могут, скачав голосовые сообщения пользователя, сгенерировать на их основе монолог для дальнейшего обмана.

Существует и другой сценарий – просьба проголосовать за детей или племянников в детском конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

В данном случае необходимо знать, что:

- не нужно переходить по неизвестным ссылкам, даже если получили их от близких или знакомых;

- при поступлении просьбы занять денежные средства в социальных сетях или мессенджерах, перезвоните своему знакомому для подтверждения информации.

7. Преступления совершены от имени государственных ведомств.

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, Росфинмониторинга, ФНС, Социального фонда России, портала «Госуслуги».

Самая распространенная уловка – предложение получить какую-либо государственную выплату.

Есть и другой сценарий. Например, звонок от представителей следственных органов или Росфинмониторинга с угрозой блокировки счета, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф. Для убедительности они могут даже прислать квитанцию на официальном бланке ведомства.

В данном случае необходимо знать, что:

- подобные ведомства не наделены полномочиями по аресту денежных средств, не оказывают платных услуг по оформлению документов, а также не рассылают подобные письма и не звонят по телефону или в мессенджерах;

- если вы получили подобные сообщения – проигнорируйте их и обратитесь напрямую в государственную организацию.

8. Преступления совершены от имени руководителя.

Злоумышленники взламывают аккаунт руководителя в мессенджере, после чего от его имени отправляют сообщения работникам с просьбой оказать помощь сотрудникам ФСБ или правоохранительным органам. В дальнейшем потерпевшему поступает звонок от неизвестного лица, которое представляется сотрудником ФСБ или правоохранительных органов и сообщает, что в бухгалтерии организации, в которой работает потерпевший, произошла утечка персональных данным и со счетов работников денежные средства переводятся на поддержку ВСУ. При этом потерпевший предупреждается об уголовной ответственности за разглашение данных предварительного следствия. После этого злоумышленники убеждают потерпевшего проследовать в банк, где необходимо осуществить снятие денежных средств с банковского счета и зачислить их на «безопасный счет», который сообщается злоумышленником для того, что бы «вычислить» недобросовестного сотрудника.

В данном случае необходимо знать, что:

- при получении подобного сообщения следует связаться с руководителем для уточнения обстоятельств;

- сотрудники полиции, ФСБ, банков никогда не звонят по вопросам сохранности сбережений;

- не существует «безопасного счета», на которые требуют перевести денежные средства.

- сотрудники полиции никогда не привлекают граждан для выявлении недобросовестного сотрудника банка.