

Информация о наиболее распространенных способах мошеннических действий

Сегодня практически каждый житель республики неоднократно слышал о мошенничествах с использованием информационно-телекоммуникационных технологий. При этом, такие преступления совершаются ежедневно.

Ежемесячно граждане переводят мошенникам свыше 220 млн. рублей.

Хуже всего то, что они попадают в долговую яму, оформляя миллионные кредиты. Ущерб от хищений с использованием ИТ-преступлений в этом году вплотную приблизился к сумме в 2 млрд. рублей (*1,98 млрд.*).

Пострадавшими от ИТ-преступлений стали более 10 тыс. граждан, которые, в большинстве случаев, имеют невысокий доход, являются работниками бюджетной сферы, пенсионерами и проявляют крайнюю доверчивость в обращении с деньгами. Порой даже не ясно о чем граждане думают, когда по указанию мошенников берут кредит в банке и переводят деньги на, так называемый, «безопасный счет».

Основная доля (*около 75%*) в общем количестве преступлений, с использованием информационно-телекоммуникационных технологий совершается с применением преимущественно двух способов – по каналам мобильной или интернет связи и при покупке-продаже различных товаров.

Наибольшую проблему для раскрытия представляют преступления, совершенные под видом телефонных звонков

сотрудников банков (около 50% от общего числа мошенничеств и краж с карт), когда злоумышленники с использованием SIP-телефонии, имитируя работу колл-центра банковского учреждения и используя терминологию сотрудников банков, вводят в заблуждение о якобы несанкционированном списании денег с банковской карты или оформлении кредитов, затем предлагают перевести деньги на «безопасный» счет, либо сообщить реквизиты банковской карты и коды подтверждения банковских операций.

В последнее время также участились случаи звонков мошенников, которые представляются должностными лицами полиции, ФСБ и прокуратуры. Вводя в заблуждение своих жертв в оказании помощи в поимке преступников, либо угрожая уголовной ответственностью за якобы совершенные переводы со счетов потерпевших за пределы Российской Федерации, они убеждают граждан перечислять свои сбережения, а нередко и заемные средства, на якобы безопасные счета.

Например, 15 сентября в Отдел полиции №7 обратился работник Территориального органа Федеральной службы по надзору в сфере здравоохранения по республике о том, что неизвестные, позвонив на сотовый телефон и представившись сотрудниками ФСБ и Центрального Банка, похитили денежные средства в сумме 1 миллиона рублей, которые он взял в кредит и перевел через банкоматы на неустановленные счета.

Более того, затем он попытался получить кредит в сумме 1 миллиона рублей в другом банке, чтобы перевести мошенникам, но

работники банка поняв, что потерпевший находится под воздействием злоумышленников вызвали сотрудников полиции.

На примере одного из руководителей Кугарчинской районной больницы можно рассмотреть типичную мошенническую схему. Так, 9 сентября ему поступает сообщение через мессенджер «Телеграмм» от неизвестного лица под именем «Булат Гарифуллин», который сообщил, что является главным врачом ГБУЗ КБ № 13 г. Уфы и пояснил, что с ним выйдут на связь сотрудники ФСБ, курирующие деятельность Министерства здравоохранения. Далее поступает звонок от якобы сотрудника ФСБ о том, что тот курирует Минздрав республики и нужно сохранить деньги потерпевшего, так как на него хотят оформить кредит и перевести деньги на Украину.

Возникает резонный вопрос: кто такой Булат Гарифуллин и почему именно он сообщает подобные новости? Почему сотрудник ФСБ звонит через Телеграмм? Как в банке можно оформить кредит без самого заявителя и уж тем более его обвинить в переводе на территорию враждебной страны, при том, что это легко проверяется?

Возвращаясь к примеру. После разговора с ФСБ происходит перенаправление потерпевшего к «специалисту» Центробанка, который говорит, что нужно опередить мошенников, то есть те кредиты, которые они хотели взять, получить самому и перевести деньги на безопасную ячейку или счет.

Для большей убедительности они направляют его в определенные отделения банков, адреса которых и фотографии есть в Интернете в свободном доступе.

В результате они, в телефонном режиме провели его по всем отделениям банков, где у него были сбережения, а также где смогли дать кредиты, убедили несколько дней прятаться и жить в гостинице в городе Салавате. По итогу было переведено на неустановленные счета 10 с половиной миллионов, из которых 8 – кредитные. Понимание ситуации пришло только после перевода денег.

Где теперь искать его деньги не ясно, мошенникам достаточно 5 минут прокрутить их на различных счетах, а нам эту цепочку раскручивать нужно больше полугода.

Отдельной проблемой является то, что большая часть персональных данных граждан, в том числе место работы, есть в сети Интернет, даже учебные заведения которые Вы закончили с профилем подготовки и годами прохождения повышения квалификации, номера СНИЛС, ИНН и даже паспортов.

А доступ к социальным сетям открывает неограниченные возможности для злоумышленников, им даже не нужно сильно стараться и они знают о Вас всю необходимую информацию, создают двойник профиля Вашего знакомого, начальника, родственника и сообщают Вам тревожную информацию.

Так, 2 октября в Отдел полиции №4 обратился профессор одного из уфимских вузов, которому в мессенджере «Телеграмм» поступило сообщение от якобы ректора о том, что с ним не могут связаться из министерства науки и образования.

Пerezвонив по указанному в сообщении номеру, он узнал, что его персональные данные попали мошенникам, в связи с чем, необходимо обналичить сбережения и перевести их на безопасные счета. Поддавшись убеждениям злоумышленников, профессор перевел на их счета более 2,5 млн. рублей.

* * *

Особую категорию потерпевших составляют желающие получить прибыль посредством инвестиций. У них, как правило, невысокий уровень образования и нет «свободных» денег.

Недостаток знаний в сфере финансовых инструментов и инвестиций, компенсируется верой в то, что за месяц можно заработать миллионы. При этом они не задаются вопросом, почему таким образом не зарабатывает остальное население или известные финансисты?

Подобные мошенничества начинаются с того, что под видом финансовых экспертов мошенники в интернете рассказывают об уникальной схеме заработка, обещают прибыль до 250% годовых, нередко возвращая незначительные суммы, заманивая граждан в свои сети.

Дизайн мошеннических сайтов похож на известные торговые площадки, сайт имитирует реальные биржи и может показывать данные реальных торгов. Между тем обычные вклады в рублях приносят от 5 до 10% годовых, самые рискованные инвестиционные паи в банках максимум 20-25% годовых. При этом после того, как потерпевший осуществит вклад денежных средств и захочет вывести прибыль, финансовые эксперты исчезают, денежные средства не возвращаются.

Например, 16 сентября в Отдел полиции №8 города Уфы поступило заявление от продавца магазина «Магнит», которая инвестировала в торговую площадку на иностранном сайте почти два с половиной миллиона рублей по совету финансового специалиста, с которым познакомилась по «Скайпу».

* * *

Особую обеспокоенность вызывает повторное появление мошенничеств под предлогом того, что родственник попал, либо спровоцировал ДТП. Несмотря на то, что способ давно известный, граждане (*в подавляющем большинстве случаев пожилые люди*), «клюют» на данную уловку. Здесь расчет сделан как раз на пожилых людей, так как звонки идут на стационарные телефоны, которыми в современном мире пользуются только пенсионеры, при этом их постоянно держат на телефоне и не дают опомниться. Злоумышленники с использованием мобильной связи, как правило, звонят на стационарный телефон пожилым гражданам, представляясь родственником, просят передать наличными денежными средствами курьерам или совершить банковские переводы за «решение вопроса» об уклонении от уголовной ответственности за якобы совершенное ДТП и компенсацию ущерба пострадавшим. Разговор с «лжеродственником» непродолжителен, затем вступает в разговор сотрудник правоохранительных органов, который подтверждает требование о вышеуказанной «компенсации».

Например, 14 марта потерпевшей возрастом более 70 лет неизвестная женщина позвонила на стационарный телефон, представившись ее дочерью, сообщила о том, что она является виновником ДТП, в результате которого пострадал другой водитель.

В ходе телефонного разговора пояснила, что договорились о денежной компенсации в размере 800 тыс. рублей, якобы на лечение пострадавших, на что потерпевшая ответила, что у нее нет таких денег, дома есть только 300 тыс. рублей наличными, упаковала денежные средства, которые позже передала неизвестному мужчине при этом не прекращая телефонного разговора.

Только передав денежные средства потерпевшая решила позвонить дочери и выяснить все ли у нее в порядке.

* * *

Как и в случае с инвестициями порой мошенники прибегают к другому способу манипуляции, под видом какого-либо крупного выигрыша, либо положенных выплат привлекают внимание доверчивых граждан.

Так, в г. Стерлитамаке 67-летней сотруднице медицинского учреждения поступил звонок якобы от сотрудников страховой компании, которые ввели ее в заблуждение и убедили перевести им сбережения. Звонившие сообщили, что горожанке положены страховые выплаты, но для того, чтобы их получить, необходимо отправить деньги за проведение финансовых операций по возмещению, и что эти средства в последующем возвратятся.

Последовав указаниям, женщина перевела более 2,5 миллионов рублей сбережений на продиктованные счета аферистов, но выплаты, разумеется, так и не получила.

При этом, встречаются случаи, когда злоумышленники предлагают вложить денежные средства, под предлогом пассивного заработка.

Например, 12 октября т.г. в отдел полиции по Туймазинскому району обратилась сотрудница одной из школ, которая перевела мошенникам 643 тыс. рублей, под предлогом получения дохода от бронирования отелей.

Аналогично в этот же день, в отдел полиции по Мелеузовскому району обратилась женщина, которой предложили заработать на проставлении оценок к фильмам на одном из интернет-кинотеатров.

В результате, злоумышленники убедили ее перевести на их счета более 1 млн. рублей (*1,1 млн. рублей*).

* * *

Также хочется отметить, что в связи со сложившейся политической ситуацией в стране и в мире, мошенники помимо хищения денежных средств, заставляют граждан выполнять определенные действия, которые могут быть уголовно наказуемыми в нашей стране.

Например, 16 мая т.г. неустановленными лицами, под видом сотрудников службы безопасности банка ПАО «Сбербанк», посредством мессенджера «WhatsApp», совершены мошеннические действия в отношении гр. «И». В последующем, они же, под предлогом возврата похищенных денежных средств, склонили гр. «И» к передаче одной из схем эвакуации цеха оборонно-промышленного комплекса и совершению поджога отделения банка в г. Уфе. После выполненных условий, гражданину «И» сообщили, что он оказал содействие сотрудникам «ЦИПСО» Украины (*Центр інформаційно-психологічних операцій — українське підрозділення ВСУ, займаючись кібератаками*).

По данному факту 26 мая т.г. в отношении гр. «И» возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 213 УК РФ (*хулиганство*).

Деньги конечно ему так никто не вернул, еще и поиздевались над его положением.

* * *

В настоящее время в связи с активным ростом рынка электронных платежей и онлайн-шопинга развиваются и новые современные формы мошенничества с использованием информационных технологий. Наиболее популярной схемой является фишинг (*англ. fishing* «рыбная ловля»). Это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей или банковским реквизитам.

Фишинг может выражаться посредством e-mail рассылок под видом известных сервисов (*социальные сети, торговые площадки*), а также при поиске информации в интернете, при переходе на которые человек попадает на сайт, внешне неотличимый от настоящего, либо на сайт с переадресацией. Когда пользователь вводит там свои данные, мошенники получают доступ к ним, после чего происходит хищение денежных средств.

Реже встречается взлом аккаунтов и рассылка от друзей с целью наживы. Мошенники пишут на электронную почту или в социальные сети родственникам и знакомым владельца страницы с просьбой срочно перевести денежные средства, придумывая различные ситуации. Зачастую потерпевшие не разобравшись в ситуации сразу же переводят деньги неизвестным лицам.

Например, в социальных сетях, рассылаются сообщения приблизительного содержания: "Привет! Проголосуй пожалуйста за Софию, это моя племяшка, участвует в конкурсе школы. Вот конкурс...".

При переходе по данным ссылкам открывается страница с вводом номера телефона и персональных данных якобы для регистрации

голосования, после чего злоумышленники получают персональные данные.

* * *

Уважаемые граждане! Для того чтобы не попасть на удочку мошенников, необходимо исключить принятие поспешных, необдуманных решений, даже если вас торопят и подгоняют с его принятием, особенно если речь о деньгах.

Если вам пришло сообщение о неожиданном списании денежных средств, не звоните по указанному в сообщении телефону и не переходите по ссылке.

Настоящий сотрудник банка и службы безопасности знают ваши фамилию имя и отчество, последние 4 цифры вашей карты и сколько на ней средств. Он не попросит снять деньги в банкомате и перевести их на другой счет. А сотрудники ФСБ и полиции не звонят используя интернет мессенджеры, не направляют скрины своих служебных удостоверений.

Кроме того финансовые организации можно проверить на официальном сайте центрального банка Российской Федерации.

А при поступлении звонков от специалистов по инвестициям, с предложением заработать, операторов сотовой связи, специалистов банка, либо госуслуг с просьбой сообщить код из СМС-сообщения, необходимо немедленно завершить разговор.