Лекции по правилам безопасности в сети «Интернет»

Мошенничество в сети «Интернет»

В настоящее время в связи с изменившимися условиями финансового рынка мошенничество в финансовой сфере зачастую связано с использованием новых механизмов и инструментов (call-центры, дроп-сервисы).

Мошенническая схема представляет собой выстроенную иерархию в виде пирамиды, на вершине которой находится организатор.

Есть так называемые «заказчики», то есть лица, имеющие большие суммы денежных средств, полученных преступным путем.

«Заказчики» подбирают «дроповодов», которые, в свою очередь, общаются с конкретными исполнителями задачи – «дропами».

«Дропы» – это подставные лица, задействованные в нелегальных схемах по выводу средств с банковских карт.

Такие лица привлекаются с целью избежать ответственности за перевод или обналичивание денежных средств со счетов и банковских карт.

К «дропам» относятся не только лица, осведомленные о противоправном характере своей деятельности, но и те, кто не понимает, что участвует в криминальной схеме.

Такие лица могут как непосредственно принимать участие в цепочке переводов или же продать (отдать) свою банковскую карточку «дроповоду» вместе с реквизитами счета и пин-кодом.

При этом сами «дропы» становятся соучастниками преступления, даже если до конца не понимают последствия своих действий. Чаще всего в «группу риска» попадают подростки, студенты, которые ищут быстрый заработок,
и доверчивые пенсионеры.

Способами привлечения подставных лиц могут быть как личные знакомства, так и обычные объявления с предложением интересной работы с предложением быстрого роста заработка.

Объявления размещаются как правило в сети Интернет, на сайтах кадровых агентств, форумах, в социальных сетях и в телеграмм-каналах.

Вместе с тем, за участие в преступных схемах в качестве «дропа» следуют неблагоприятные последствия, поэтому если Вы случайно стали участником нелегальной схемы, следует заявить об этом в правоохранительные органы.

Так, банками непрерывно проверяются операции в целях выявления клиентов с признаками «дроппа», указанные клиенты ставятся на дополнительный учет, вводятся ограничения на получение новых карт, иных электронных средств платежа и на проведение финансовых операций по выпущенным картам.

При выявлении банками состава и участников дроп-схемы по обналичиванию денежных средств информация о таких клиентах и операциях направляется в правоохранительные органы.

Участие в преступных схемах в качестве «дропа» влечет уголовную ответственность, в том числе по статьям 187 (неправомерный оборот средств платежей), 159 (мошенничество) Уголовного кодекса Российской Федерации. Помимо этого, за указанные действия в соответствии с гражданским законодательством граждане несут финансовую ответственность.

Если Вы все-таки стали жертвой злоумышленников, постарайтесь как можно скорее обратиться в ближайший отдел полиции или позвонить по телефону 02 (с мобильного 102).

Ответственность за незаконный оборот средств платежей (банковских карт)

За сбыт средств платежей (банковских карт) граждане несут уголовную ответственность по статье 187 Уголовного кодекса Российской Федерации.

Санкция статьи предусматривает ответственность в виде принудительных работ на срок до пяти лет либо лишения свободы на срок до шести лет со штрафом в размере от 100 тысяч до 300 тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

Если данное преступление совершено группой лиц, то наказание может быть назначено в виде принудительных работ на срок до пяти лет либо лишения свободы на срок до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет или без такового.

Зачастую указанные средства платежей передаются гражданами третьим лицам по их просьбе и за обещанное ими вознаграждение.

Гражданами передаются как уже имеющиеся у них в распоряжении банковские карты, так и открытые в банковских учреждениях по просьбе тех же третьих лиц.

Средства платежей используются при транзитном перечислении на них денежных средств со счетов «фирм-однодневок» и последующем их обналичивании с целью придания им законного характера получения.

Помимо этого, за указанные действия в соответствии с гражданским законодательством граждане несут финансовую ответственность.

В судебном порядке в доход государства взыскиваются денежные средства, полученные за открытие банковских счетов и передачу банковских карт в пользование иным лицам.

Нередко утеря или предоставление гражданами своих паспортных (персональных данных), банковских карт могут быть использованы неизвестными лицами в преступных схемах, что может повлечь для их владельцев наступление финансовой ответственности.

Так, решением областного суда Челябинской области с гражданина, нарушившего правила банковского обслуживания, передавшего свою

банковскую карту третьим лицам, взыскано 300 тыс. рублей, поступивших на его счет от потерпевшей, перечисливших их под влиянием мошенников.

Телефонное мошенничество

Действия телефонных мошенников квалифицируются по ст. 159 Уголовного кодекса как мошенничество, т.е. умышленные действия, направленные на хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При этом под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества (п. 1 примечаний к ст. 158 УК РФ).

Задачей телефонного мошенника является узнать у гражданина номера, коды, пароли и другие реквизиты банковских карт, а также убедить оформить кредит или снять денежных средств и передать их постороннему лицу.

Следует учитывать, что талантливые мошенники владеют даром убеждения и в совершенстве используют приемы психологического манипулирования. Путем введения человека в паническое состояние они провоцируют гражданина на срочность совершения платежа, оформления кредита или снятия денежных средств.

Для того, чтобы не стать такой жертвой, необходимо следовать определенным правилам:

- если получен звонок с просьбой о срочной денежной помощи для известного гражданину лица (знакомого, родственника и т.п.), следует не принимать решение сразу, идя на поводу у позвонившего, а проверить полученную от него информацию, перезвонив вышеуказанным лицам, или связаться с ними иными способами;

- нельзя сообщать по телефону личные сведения или данные банковских карт, которые могут быть использованы злоумышленниками для неправомерных действий;

- нельзя перезванивать на номер, если он незнаком, и т.п.

Если гражданин предполагает, что стал жертвой телефонного мошенничества, ему необходимо обратиться в органы внутренних дел с соответствующим заявлением. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Кроме этого, следует сообщить о факте телефонного мошенничества в абонентскую службу мобильного оператора, который обслуживает номер преступника. Если гражданин, к примеру, совершил перевод денежной суммы по мобильной сети, то принятие оператором экстренных мер может позволить заблокировать перевод и вернуть деньги.

Правила безопасности в сфере противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий

Мошенниками разработано множество схем хищения денежных средств путем обмана или злоупотребления доверием:

– звонки с сообщением о мошеннических действиях с личным кабинетом на сайте Госуслуг;

– сообщение о подозрительных операциях с банковскими счетами, где в ходе разговора жертва переводит денежные средства на несуществующий «безопасный счет»;

– сообщение о подозрительных операциях с банковскими счетами, где для предотвращения хищения денежных средств необходимо установить специальную программу на мобильный телефон, а также зайти в приложение банка, после чего мошенник получает удаленный доступ к приложению банка, оформляет кредит и выводит денежные средства со счета жертвы;

– звонки «родственник в беде» - сообщение об участии родственника в дорожно-транспортном происшествии и его виновности в нем, о необходимости передачи денежных средств для оказания помощи пострадавшим и избежания привлечения родственника к уголовной ответственности;

– размещение в сети Интернет информации с предложением дополнительного «легкого» заработка путем ставок на бирже, в результате чего жертвы перечисляют свои личные сбережения на специальный счет, однако обратно получить их не могут, все денежные средства «уходят» на счета мошенникам.

Несмотря на многочисленные предупреждения правоохранительных органов, количество зарегистрированных сообщений о хищении денежных средств с использованием мобильной связи и сети Интернет растет, люди продолжают доверять незнакомцам по телефону.

Еще одна схема мошенников - извещение об истечении срока действия договора об оказании услуг мобильной связи.

Злоумышленник звонит жертве представляясь «оператором сотовой связи», сообщает о необходимости продления договора, для чего необходимо сообщить код из смс сообщения.

Далее жертве приходит уведомление о совершении входа в личный кабинет на сайте Госуслуг, где указан телефон службы поддержки. Жертва обращается в «службу поддержки», где ей сообщают о том, что с использованием ее персональных данных поданы заявки на оформление кредитов, в целях исключения возможности воспользоваться данным кредитом мошенники, уверяют жертву о необходимости оформления аналогичного кредита и перевода его на номер карты, который они укажут. Введенные в заблуждение граждане самостоятельно оформляют кредит, а

затем переводят полученные денежные средства на счет, который был указан мошенником.

Чаще всего подобные телефонные разговоры осуществляются посредством интернет мессенджеров (WhatsApp, Telegram). Сотрудники каких-либо организаций не осуществляют звонки через указанные мессенджеры.

Если Вам звонит «сотрудник банка» и сообщает о списаниях денежных средств с Вашего счета, о взломе Вашего личного кабинета или о попытке оформления кредита, «сотрудник оператора сотовой связи» о необходимости продления договора, «сотрудник правоохранительного органа» с сообщением о мошеннических действиях с вашими банковскими счетами - незамедлительно кладите трубку, независимо с какого номера телефона поступил звонок.

Для проверки информации перезвоните в банк, оператору сотовой связи либо в правоохранительный орган самостоятельно. Не производите никаких действий с банковской картой по указанию третьих лиц.

Так как за совершение данных незаконных действий предусмотрена уголовная ответственность, по статье 159 УК РФ, в случае если вы стали жертвой мошенников, обращайтесь с заявлением в органы полиции по месту совершения преступления.

«Дроппер» как участник мошеннической схемы

В условиях современного мира разновидность кибермошенничеств - преступлений с использованием IT-технологий, весьма обширна. Данные преступления тщательно спланированы и, как правило, совершаются подготовленной организованной преступной группой на протяжении длительного периода времени. Одним из этапов совершения кибермошенничеств является обналичивание доходов, полученных преступным путем через «дропперов» (сокращенная версия термина – «дропы»).

Уровень автоматизации процессов в банковской сфере позволяет мошенникам для денежных транзакций использовать банковские счета, открытые на физических лиц («дропов»), и их электронные кошельки. Высокая скорость исполнения денежных транзакций дает возможность мошенникам практически одновременно с переводом денежных средств снимать их через банковские терминалы и смарт-терминалы.

Как правило они получают вознаграждение за выполнение определенных поручений по обналичиванию, при этом могут быть введены в заблуждение, не знать о мошенническом характере действий и стать соучастником преступной схемы.

В целом работа «дропа» заключается в том, что на его банковскую карту поступают средства, которые он должен передать другому участнику цепочки, либо перевести на другой счет, либо обменять на криптовалюту, либо другой наиболее распространённый вариант «дропперства»: человек

передает мошенникам свою банковскую карту или предоставляет доступ в личный кабинет интернет-банка.

Одним из способов вовлечения в совершение преступления может быть даже просьба у банкомата снять наличные средства под предлогом потери карты: злоумышленник переводит деньги на карту жертвы, которая ничего не подозревая, их обналичивает.

В настоящее время на столбах, подъездах, остановках появились объявления о покупке дебетовых карт. Граждане, думая в том, что передают сведения не кредитной, а дебетовой карты, считают, что защищены от оформления кредитов на свое имя. Желая получить «заработок», передают своибанковские карты, не осознавая меру своей финансовой ответственности,
которая зависит от того, какие операции будут проведены по купленным у них банковским картам.

При этом каждый владелец карты несет ответственность за все совершенные операции, неважно кто их проводит.

В силу статьи 8 Гражданского кодекса Российской Федерации (далее – ГК РФ) гражданские права и обязанности возникают из неосновательного обогащения.

Согласно статье 1102 ГК РФ лицо, которое без установленных законом, иными правовыми актами или сделкой оснований приобрело или сберегло имущество (приобретатель) за счет другого лица (потерпевшего), обязано возвратить последнему неосновательно приобретенное или сбереженное имущество (неосновательное обогащение).

При этом данные правила применяются независимо от того, явилось ли неосновательное обогащение результатом поведения приобретателя имущества, самого потерпевшего, третьих лиц или произошло помимо их воли.

По делам о взыскании неосновательного обогащения обязанность доказать наличие законных оснований для приобретения или сбережения такого имущества возлагается на владельца банковской карты.

Таким образом, «дроппер», передав свою карту злоумышленнику за вознаграждение, рискует стать ответчиком по гражданскому делу о взыскании неосновательного обогащения на всю сумму проведенных финансовых операций по его карте. А в случае осведомленности «дроппера» о преступном характере совершаемых действий по его карте, последний может быть привлечен к уголовной ответственности за совершенное преступление.

В Пермском крае сложилась положительная практика предъявления органами прокуратуры края гражданских исков к «дропперам» о взыскании неосновательного обогащения, поскольку их причастность к совершению незаконных финансовых операций, подтверждается банковскими документами, даже в том случае, если виновное лицо (организатор) преступления не установлен.

Получение информации о владельце банковского счета для правоохранительных органов не представляет сложности, то есть выявление

«дропа» и привлечение его к установленной законодательством ответственности вопрос времени.

Распространенные способы мошенничества с применением информационно-телекоммуникационных технологий В условиях современного мира разновидность преступлений с использованием IT-технологий, весьма обширна. Такие преступления тщательно спланированы и, как правило, совершаются подготовленной организованной преступной группой на протяжении длительного периода времени.

Вот наиболее распространенные из них:

1. Злоумышленники, доподлинно зная о том, что их жертва трудоустроена в какой-либо организации, создают клон страницы в социальной сети (Вконтакте, Telegram, Whatsapp) руководителя данной организации, после чего от его лица сообщают гражданину о якобы проводимой в их организации проверки ФСБ России факта перечисления сотрудниками организации денежных средств в поддержку Вооруженных Сил Украины.

После сообщения данного факта жертве непременно звонят якобы сотрудники ФСБ России и сообщают, что с их банковских счетов осуществляются переводы денежных средств на нужды Вооруженных Сил Украины.

Патриотически-настроенные граждане, думая о том, что их деньги могут оказаться в руках противника, выполняют все указания мошенников.

Для того, чтобы не стать жертвой такой схемы мошенничества, следует немедленно прекратить телефонный разговор, уведомить руководителя о получении указаний от его лица через социальную сеть, предупредить других сотрудников об этой ситуации. При необходимости через приложение банка заблокировать доступ к своим банковским счетам и обратиться в органы полиции.

2. Гражданину в социальной сети или интернет-мессенджере (ВКонтакте, Telegram, WhatsUp) приходит сообщение от клона профиля знакомого ему лица с текстовым сообщением «Это твои фотографии?/Это ты на видео?/Ты знаешь этого человека?» с приложением ссылки или стороннего файла любого другого формата.

Текст сообщения может варьироваться. В любом случае содержание такого сообщения направлено на побуждении интереса у лица к открытию и прочтению сообщения.

При последующем открытии приложенной ссылки или стороннего файла происходит автоматическое скачивание вредоносного приложения, которое предоставляет мошенникам полный дистанционный доступ к мобильному устройству гражданина, что и позволяет в последующем осуществить хищение принадлежащих ему денежных средств.

Чтобы обезопасить себя от такого типа мошенничества следует помнить, что открывать диалоговое окно с приложенным файлом или ссылкой безопасно, но в последующем следует детально изучить полученное сообщение: установить, является ли профиль отправителя «подлинным», проверить контактны данные, обратить внимание на отсутствие в диалоге

иных сообщений и медиа-файлов; обратить внимание на текст ссылки и формат приложенного файла. Следует остерегаться форматов «exe». Зачастую мошенники прикладывают файл с наименованием «mamont». В случае открытия вредоносного файла мобильное устройство начнет производить самостоятельные бесконтрольные действия. Попробуйте незамедлительно выключить его длинным нажатием клавиши «блокировка» или физическим извлечением батареи. Если мошенникам все же удалось похитить денежные средства незамедлительно обращайтесь в полицию. Ни в коем случае не форматируйте мобильное устройство, оставшиеся на нем сведения важны для осуществления расследования.

3. Мошенничество в популярных среди детей онлайн играх, примером служит игра Roblox (роблокс).

В ходе игры детям предлагается подписаться на страницу в социальной сети Телеграмм, где разыгрывается пополнение игрового счета. Для перечисления выигрыша, злоумышленники просят ребенка сфотографировать банковское приложение в телефоне родителей (сфотографировать банковскую карту, осуществить перевод денежных средств через приложение банка и пр.), требуют это сделать незамедлительно, объясняя тем, что приз скоро исчезнет.

После того, как ребенок выполнит указания, денежные средства со счета родителей уходят к мошенникам. В основном в такую ситуацию попадают дети в возрасте от 7 до 12 лет. Дети этого возраста уже разбираются в компьютерной технике, смартфонах и соцсетях. Если в семье не выстроен доверительный диалог, велика вероятность, что ребенок без спроса возьмет телефон/банковскую карту родителей чтобы получить как можно скорее заветный приз.

Родителям важно защитить детей от мошенников. Необходимо проверять приложения, которые использует ребенок, разговаривать с ним об угрозах в сети и правилах безопасного поведения в интернете. Необходимо объяснить ребенку, что вводить данные банковских карт или делиться иной личной информацией в интернете нельзя.