**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 «дропа», 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.

**Памятка пожилым гражданам «Как не стать жертвой мошенников»**

Так, чтобы не стать жертвами разных видов мошенничества в сети «Интернет» и с использованием различных информационных технологий необходимо знать следующее:

— представители госучреждений никогда не звонят, чтобы сообщить узнать какую-либо персональную информацию о вас (данные паспорта, банковских карт, код доступа к кредитной карте и тп);

— если звонящий называет Вас по имени и отчеству и знает ваш адрес, семейное положение и другую информацию, это вовсе не означает, что он является официальным лицом (такие данные можно получить разными способами), спросите имя, фамилию и занимаемую должность звонящего, перезвоните в организацию и убедитесь в том, что Вас не обманывают;

— если по телефону Вам звонит близкий человек (сын, внук, внучка и т.д.), говорит, что попал в беду, и просит прислать денег через курьера или перевести на какой-то счет, не спешите этого делать, перезвоните звонившему, а если он не возьмет трубку, наберите другим родственникам;

— чтобы пенсионер смог получить социальные выплаты, работники территориальных Социального фонда Российской Федерации никогда не потребует переводить деньги на какой-либо счет;

Также одним из распространенных видов мошенничества является розыгрыш призов, когда мошенник сообщает Вам, что Вы выиграли ценный приз, но существует один маленький нюанс - для получения приза необходимо оплатить налог на выигрыш либо оплатить его доставку. Этого делать нельзя, после перехода по ссылкам списываются денежные средства с привязанных карт и счетов номеров телефонов.

Также может приходить сообщение о том, что Ваша банковская карта заблокирована и предлагается бесплатно позвонить на определенный номер для получения подробной информации. Не торопитесь звонить по указанному телефону. Чтобы похитить Ваши денежные средства, злоумышленникам нужен номер Вашей карты и ПИН-код, для этого они могут сказать, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. Как только Вы их сообщите, деньги будут сняты с Вашего счета.

Не сообщайте реквизиты Вашей карты, ни одна организация, включая банк, не вправе требовать Ваш ПИН-код. Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

**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.

Только за 2023 год по 18 материалам прокурорских проверок правоохранительными органами Пермского края возбуждено 15 уголовных дел по статье 187 Уголовного кодекса Российской Федерации.

В частности, в Уинском муниципальном округе возбуждено и расследуется уголовное дело по факту открытия гражданином банковского счета по просьбе третьего лица на безвозмездной основе и передачи последнему банковской карты в пользование.

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

В текущем году органами прокуратуры края с граждан в судебном порядке в доход государства взыскивались денежные средства на общую сумму 17 тыс. рублей, полученные ими за открытие банковских счетов и передачу банковских карт в пользование иным лицам.

Например, по иску прокуратуры г. Гремячинска решением Губахинского городского суда с жителя г. Гремячинска взысканы 2 тыс. рублей, полученные им от другого лица за открытие счетов в 3 различных банках и последующую передачу этому лицу в пользование банковских карт.

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, по иску прокуратуры Свердловского района г. Перми решением Верхнеуральского районного 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.

**Видеоролики на платформе «Яндекс Диск»:**

https://disk.yandex.ru/i/WaxOnz8zzDpXQQ;
https://disk.yandex.ru/i/VgQM6cWLVCat8g;
https://disk.yandex.ru/i/I06gdo2qjz7PAQ;
https://disk.yandex.ru/i/VieGq2HBFI9bcg.

**Список интернет-ресурсов Банка-России, Минцифры России, МВД России, финансово-кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности, содержащих информационно-разъяснительные материалы по профилактике дистанционных преступлений**

**МВД России:**
https://МВД.рф/Videoarhiv/Socialnaia reklama;
https:// МВД.рф/mvd/structure1/Upravfenija/убк;
t.me/cyberpo ice_rus.

**Банк России:**
cbr.ru/protection_rights/finprosvet;
vk.com/cbr_official;
t.me/centralbank_Russia;
https://dni-fg.ru/;
https://fincult_info;
https://doligra.ru;
t.me/fintrack cbr;
t.me/fincult_ihfo;
vk.com/finprosv.

**Минцифры России:**

https://www.gosuslugi.ru/cybersecurity;
https://киберзож.рф/;
https://выучисвоюроль.рф;
https://прокачайскиллзащиты.рф;
https://готовкцифре.рф;
t.me/mintsifry.

**Интернет-ресурсы финансово-кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности:**

https://www.sberbank.ru/ru/person/kibrary;
https://learn.vtb.ru/fingram/;
https://megafon.ru/help/antifraud/;

https://kaspersky.ru/resource-center;
https://kids.kaspersky.ru/;
https://rocit.ru.