**Информация**

**о наиболее распространенных способах совершения преступлений**

**с использованием информационно-телекоммуникационных технологий**

1. Мошенническая схема остается предлог дополнительного заработка, участия в торгах на бирже, а также инвестирования в различные ценные бумаги. Граждан заманивают яркими вывесками, наименованиями, созвучными с названиями крупных нефте-газодобывающих компаний и холдингов, так называемыми «исключительными» предложениями и возможностью получения высокого дохода, в том числе за короткий промежуток времени. Попавшего под воздействие указанных факторов человека вынуждают вносить крупные суммы денежных средств, без возможности их вывода в дальнейшем.

2. Распространение получила схема хищения денежных средств с использованием социальных интернет-сетей. Якобы от имени потерпевшего его знакомым, друзьям, родственникам приходит сообщение с просьбой одолжить денежные средства. Также злоумышленники с использованием популярных мессенджеров рассылают сообщение о сборе денежных средств на лечение больного ребенка, похороны и т.д.

3. Действует преступная схема с оформлением кредита в микрофинансовых организациях без ведома потерпевшего. Хищение осуществляется путем перебора сим-карт для поиска активного аккаунта заемщика и использование личного кабинета лица, ранее оформлявшего в микрофинансовых организациях заем.

4. Еще одним способом остается совершение противоправных деяний под предлогом получения возврата (компенсации) денежных средств за ранее приобретенные биологически активные добавки (БАДы). Мошенники, представляясь сотрудниками правоохранительных органов, в телефонном разговоре с потерпевшим сообщают, что задержали преступников, занимавшихся ранее продажей некачественных пищевых добавок. Для получения компенсации необходимо оплатить налог, открыть счет, совершить транзакцию и т.п. В результате граждане, рассчитывая получить компенсацию, перечисляют мошенникам денежные средства, сумма которых превышает сумму обещанной компенсации.

5. Электронные письма на почту, которые приходят от «центра обмена сообщениями хостинга веб-почты», то есть от несуществующей организации. Авторы рассылки сообщают, что обновляют базу и удаляют все неиспользуемые учетные записи. Они настоятельно рекомендуют подтвердить электронную почту и обновить данные - так они будут знать, что аккаунт активен, и не будут его удалять. При этом не используются вредоносные программы и фишинговые сайты, необходимую мошенникам информацию (имя, фамилию, логин и пароль) просят прислать ответным сообщением. Таким образом мошенники получают доступ к личным данным граждан.

6. Мошенники стали чаще подделывать банковские приложения, например «Сбер 2.0» и «Поддержка Сбербанка». Злоумышленники звонят клиентам от имени сотрудника «Сбера» и убеждают установить приложения «Сбер» или «Поддержка Сбербанка». На самом деле под видом этих приложений киберпреступники распространяют программы для удаленного доступа к устройствам. Если пользователь установит одно из таких псевдо приложений, мошенники похищают его личную информацию и деньги с банковских карт.

7. Новые функции в телеграм-каналах – возможность публиковать сторис. Для этого необходимо получить определенное количество голосов «бустов» (голосов). В связи с этим появились чат-боты, предлагающие купить «бусты» в больших количествах. Вводить данные банковской карты при этом не надо – просят выслать деньги обычным переводом. Пользователь переводит деньги, но по сути, не получает никаких гарантий, при этом у бота нет формы обратной связи.

8. Злоумышленники звонят от имени руководства компаний, организаций. Представляясь генеральным директором, мошенники предупреждают служащих, что им скоро поступит телефонный звонок от представителя курирующего эти компании Министерства. При этом, в мессенджерах используются аккаунты с реальными фотографиями и ФИО руководителей компаний, организаций. Далее действительно поступает звонок, в ходе разговора мошенники под различным предлогом получают конфиденциальную информацию, с целью совершения мошеннических действий.

9. Рассылка в социальных сетях и мессенджерах сообщений с предложением проголосовать по различным темам (участие в конкурсе, выбор музыкальной композиции, фильма и т.п.), содержащих ссылку, после перехода по которой легальный аккаунт пользователя перехватывается злоумышленниками. В этом случае необходимо при восстановлении доступа к аккаунту использовать штатные механизмы социальной сети и мессенджера.

10. Мошенничество, совершаемое посредством подменной телефонии. Мошенник звонит потерпевшему с подменных номеров (номерная емкость начинается с 8800, 495, 499, а также с использованием номеров телефонов реально существующих ведомств, организаций, государственных органов, применяя специальное оборудование), представляясь сотрудником банка, полиции, прокуратуры, ФСБ, Следственного комитета, информирует гражданина о подозрительных финансовых операциях по его банковского счету, попытках оформления кредита, перевода денежных средств со счёта, либо сообщает о розыске, задержании преступников, совершающих хищения денежных средств с расчетных счетов граждан, при этом извещает о необходимости соблюдения «тайны следствия». Далее мошенник, используя методы психологического воздействия и пользуясь доверчивостью граждан, вынуждают потерпевшего сообщать персональные данные, сведения о финансовом состояния, о наличии автотранспорта в собственности. Затем под манипулятивным воздействием мошенника, потерпевший переводит денежные средства на якобы безопасные расчетные счета (в отдельных случаях, переводя деньги, вырученные от срочной продажи автотранспорта. Сделку по срочной продаже автотранспорта организуют сами мошенники). Потерпевшие: все категории граждан, независимо от пола, образования, экономического, национального, социального статуса, а также возраста.

11. Мошенничество, совершаемое под предлогом оказания содействия родственнику, якобы попавшему в дорожно-транспортное происшествие или якобы задержанному правоохранительными органами. Денежные средства потерпевший передает прибывшему к нему курьеру, который в дальнейшем перечисляет полученные денежные средства на указанные мошенниками банковские счета, при этом 15% оставляя себе. Потерпевшие: основная часть – пожилые люди.

12. Мошенничество, совершаемое под предлогом дополнительного заработка, участия в торгах на бирже, инвестирования в ценные бумаги. Граждан заманивают яркими вывесками, названиями созвучными с названиями крупных нефте/газодобывающих компаний и холдингов, таких как Газпроминвестии, ТинькоффИнвест, «исключительными» предложениями, возможностью получения высокого дохода, вынуждают потерпевшего вносить крупные суммы, без возможности вывода денежных средств в дальнейшем. Потерпевшие: все категории граждан, независимо от пола, образования, экономического, национального, социального статуса, а также возраста.

13. Мошенничество с использованием торговых площадок Авито, Юла, объявлений о купле/продаже в социальных сетях:

- путем размещения «липового» объявления о продаже товара по цене значительно ниже рыночной. Как правило, переписка между покупателем и мошенником ведется на торговой площадке либо с использованием мессенджеров WhatsApp, Telegram, Viber. В ходе общения мошенник «втирается» в доверие и вынуждает жертву оплатить товар полностью либо внести предоплату путем электронных переводов. После оплаты контакты с покупателем прекращаются, его блокируют, объявление удаляют.

- хищения денежных средств под предлогом покупки товара. В данном случае переписка между продавцом и мошенником также ведется с использованием сообщений на сайте, либо с использованием мессенджеров WhatsApp, Telegram, Viber. Продавца убеждают направить товар Авито, Юла доставкой, сообщая, что товар оплачен, и для получения денежных средств необходимо перейти по ссылке, которую скидывают на телефон продавца. После перехода по ссылке продавец попадает на фишинговый сайт Авито, Юла, где вносит свои персональные данные и реквизиты банковской карты, сумму для получения. После нажатия на «окно» «Получить деньги», денежные средства списываются с расчетного счета продавца. Кроме того, в дальнейшем мошенники убеждают продавца, что произошел сбой и для возврата денежных средств необходимо обратиться в службу поддержки, перейдя по ссылке. Продавец, перейдя по ссылке, вновь попадает на фишинговый сайт, где указывает свои данные, реквизиты карты и сумму, якобы необоснованно списанную. После нажатия на «окно» получить деньги, с расчетного счета продавца повторно списываются денежные средства.

14. Сайт по поиску попутчиков («BlaBlaCar»): мошенники размещают на сайте объявления с предложением услуги по пассажироперевозке. Когда пользователь откликается на объявление, мошенник в чате на сайте BlaBlaCar просят его связаться с ним в WhatsApp по определённому номеру телефона. Затем, в ходе переписки в WhatsApp клиенту предлагают оплатить поездку и скидывают ему ссылку на фишинговый сайт для оплаты поездки. После перехода на сайт, пользователь вводит реквизиты своей банковской карты, далее денежные средства списываются на счёт мошенники.

15. «Оформлена заявка на кредит».

Если Вы не обращались в банк, а Вам сообщают о предварительно одобренном кредите – положите трубку, это мошенники. Не продолжайте разговор, иначе в ходе телефонного разговора под психологическим давлением, Вы рискуете потерять деньги.

16. «Сотрудник Центробанка».

Сотрудники Центрального Банка Российской Федерации не звонят клиентам и не пишут СМС-сообщения для совершения каких-либо банковских операций, если абонент представляется сотрудником Центробанка – прекратите разговор, положите трубку.

17. «Специальный безопасный счет».

Это распространенная схема мошенников, убеждающих граждан перевести свои сбережения на «специальные безопасные счета», под легендой сохранности денежных средств. Специальных и каких-либо безопасных счетов не существует, если Вас просят перевести деньги на такие счета – прекратите разговор, положите трубку.

18. «Идут следственные действия, помогите задержать мошенников».

Сотрудники правоохранительных органов не проводят процессуальные действия по телефону, не запрашивают финансовые данные и не предлагают поучаствовать в задержании преступников.

19. «Зафиксирована подозрительная операция».

Банки могут приостанавливать такие операции без участия клиента. Если у банка возникнут сомнения, Вам позвонят с официального номера или напишет служба поддержки через соответствующее приложение банка (программу) для современных средств коммуникации. Вместе с тем, сотрудник банка никогда не будет просить переводить деньги, а только лишь удостоверится, что Вы действительно совершаете перевод.

20. «Срок действия сим-карты истекает».

Если поступает такой звонок, положите трубку. У сим-карты операторов связи отсутствуют ограничения по срокам их использования.

21. «Продиктуйте код из СМС-сообщения».

Код из СМС-сообщения, поступившего из банка или с интернет-портала «Госуслуги» – это информация для персонализированного доступа, его никому и никогда сообщать нельзя, даже сотрудникам банка.

**ГУ МВД России по Челябинской области сообщает, что если в ходе телефонного разговора с Вами заговорили о деньгах и счетах, просят куда-либо перевести сбережения – положите трубку, самостоятельно наберите телефон банка или полиции.**

*ГУ МВД России по Челябинской области*

*Аппарат межведомственной комиссии по профилактике правонарушений на территории Копейского городского округа*