Отвечая на поставленные вопросы, следует отметить, что мошенники умело пользуются малой информированностью участников СВО, а также сложной морально-психологической ситуацией родственников, у которых отсутствует прямая связь с военнослужащими.

Высокая концентрация денежных средств и значительность сумм единовременных выплат является привлекательной для злоумышленников мишенью.

Анализ уголовных дел показывает, что ***действия злоумышленников по обману участников СВО и их близких можно разделить на следующие популярные способы:***

1. Злоумышленники создают каналы в мессенджере Telegram, визуально похожие на официальные группы, посвященные помощи семьям военнослужащих, в которых регулярно публикуют сведения о пропавших военнослужащих, их фотографии, а также PDF- и Excel- файлы с персональными данными.

В те же каналы начинают позднее загружать вредоносное программное обеспечение (например APK-файлы, содержащие банковский «троян» Mamont для операционной системы Android).

Используя данный «вредонос» злоумышленники получают полный контроль над устройством жертвы, могут собирать о нем информацию, перехватывать и отправлять СМС, получить доступ к пользовательским контактам и т.д., а также банковским приложениям и мессенджерам.

В целях безопасности необходимо отключить автозагрузку в Telegram, проверять формат документов.

2. Помощь в оформлении выплат, как способ войти в доверие.

Так, в сентябре текущего года возбуждено уголовное дело по факту мошенничества в отношении вдовы участника специальной военной операции.

Инцидент начался с телефонного звонка, в ходе которого неизвестный поинтересовался, получала ли женщина причитающиеся ей выплаты и награду погибшего супруга.

После отрицательного ответа злоумышленник предложил оформить необходимые документы через портал «Госуслуги» и под предлогом оказания помощи запросил у нее код подтверждения из СМС-сообщения.

Впоследствии, лже-сотрудник правоохранительных органов обвинил женщину в соучастии в мошеннической деятельности и пригрозил уголовным преследованием. Под давлением мошенников жертва передала все имеющиеся денежные средства неизвестному курьеру, прибывшему по ее месту жительства.

В целях безопасности:

- никому и никогда не передавайте коды из СМС-сообщений;

- не переходите по ссылкам из сообщений и не устанавливайте программное обеспечение из непроверенных источников;

- разумно подходите к публикации в социальных сетях личной информации, так как она может стать информацией, необходимой мошеннику для создания сценария обмана.

3. Мошенники звонят или пишут своим потенциальным жертвам и сообщают, что из их денежного довольствия будет удержано 195 000 рублей – размер единовременной выплаты, которая причитается военным в соответствии с указом Президента РФ. Причина – дисциплинарное взыскание. Для большей убедительности мошенники направляют в мессенджер «копию выписки» якобы из приказа Департамента финансового обеспечения Минобороны России.

Чтобы денежные средства не были списаны, мошенники предлагают военнослужащему или его родным перевести все накопления якобы на «безопасный счет». Получив деньги жертвы, телефонные аферисты исчезают.

Как себя обезопасить:

- если Вам поступил подозрительный звонок, прервите разговор, положите трубку;

- не забывайте, что «безопасных счетов» не существует;

- по всем вопросам, связанным с денежными средствами, обращайтесь в свой банк самостоятельно.

4. «Хищение денежных средств с банковских счетов военнослужащих, в том числе получивших ранение или погибших в зоне проведения СВО».

Военнослужащие хранят свои банковские карты в открытых местах, сохранность личных вещей ими никак не обеспечена.

В результате этого каждый может получать доступ к их вещам, что ведет в дальнейшем к хищению денежных средств.

Ярким примером может послужить совершенное в декабре 2024 года хищение денежных средств с банковского счета одного из военнослужащих, который погиб в зоне проведения СВО, в общей сумме более 2 млн рублей.

Похищенные денежные средства обналичены неустановленными лицами в декабре 2024 года через банкоматы, расположенные в Луганской Народной Республике. О хищении денежных средств, в том числе суммы единовременной выплаты за гибель, мать погибшего узнала при вступлении в наследство.

Аналогичным способом похищены денежные средства в общей сумме более 1 млн рублей с банковского счета еще одного из военнослужащих, который получил ранение в зоне проведения СВО и находился на лечении.

Во всех этих случаях вывод похищенных денежных средств мошенниками осуществляется путем несанкционированного доступа к банковским счетам военнослужащих посредством утраченных ими мобильных телефонов с установленными в них мобильными приложениями банков и выманенных у жертвы реквизитов карты, CVV-кодов, паролей из SMS и кодов из push-уведомлений.

Как подготовиться к такой ситуации заранее:

- не носите с собой банковские карты, оставьте их в безопасном месте;

- не храните вместе с банковской карты ПИН-код;

- включите все уведомления (СМС и Push- уведомления) на Все операции по карте;

- помните, что мобильный телефон с банковским приложением может быть также Вами утерян;

- установите лимиты на снятие наличных, на безналичную оплату и онлайн-платежи на комфортный для Вас уровень (к примеру, 5 000 рублей в день). Сделать это можно в мобильном приложении банка;

- используйте виртуальную карту для онлайн-платежей.

В целях безопасности после обнаружения утери банковской карты:

- откройте мобильное приложение банка и выберите опцию «Заблокировать карту»;

- если нет доступа к приложению, немедленно позвоните на горячую линию банка по номеру телефона, указанному на официальном сайте.

Подобные преступления находятся на особом контроле у правоохранительных органов. По фактам хищений возбуждаются уголовные дела, и виновные несут суровые наказания. Однако проблема требует комплексного решения, включающего как технические меры защиты, так и повышение финансовой грамотности населения.

Одновременно, в целях противодействия совершения отмеченного вида преступлений, будем признательны за участие в распространении среди военнослужащих и членов их семьи дополнительной информационно-профилактической продукции, наиболее приемлемыми и легкоусвояемыми формами восприятия которой являются просмотр фото и видеоконтента на различных интернет-площадках, социальных сетях и средствах массовой информации, а также проведение очных лекций в коллективах.

Рекомендуется использовать рубрику сайта Следственного департамента МВД России «Профилактика мошенничества». В разделе «Новости» размещено 353 информационных сообщений о дистанционных хищениях.

Также соответствующие профилактические материалы и видеоконтенты содержатся на ресурсах, посвященных недопущению преступлений в отношении граждан, ознакомиться с которыми можно по ссылкам:

https://мвд.рф/вопросы/мошенник и https://мвд.рф/news/rubric/17 *(официальные интернет-сайты МВД России)*;

https://мвд.рф/Videoarhiv/Socialnaja_reklama/вбезопасности/item/55246013/

https://мвд.рф/Videoarhiv/Socialnaja_reklama/вбезопасности/item/54619404/

https://мвд.рф/Videoarhiv/Socialnaja_reklama/вбезопасности/item/5461707

(видеоконтенты: «рекомендации для граждан о навыках безопасности при использовании банковских карт, интернет-банкинга, банкоматов», «звонок от «оператора сотовой связи», «звонки от сотрудников государственных органов», «что такое фейковые QR-коды и как этим пользуются мошенники?»);

https://мвд.рф/mvd/structure1/Upravlenija/убк/информация-для-граждан *(официальный интернет-сайт УБК МВД России)*;

https://t.me/cyberpolice_rus *(официальный телеграм-канал УБК МВД России)*;

https://www.kaspersky.ru/ *(официальный интернет-сайт компании «Лаборатория касперского»)*;

https://www.securitylab.ru/ *(информационный портал по безопасности)*;

https://ligainternet.ru/ (официальный *интернет-сайт компании «Лига безопасного интернета»)*;

https://t.me/internetinsafe *(официальный телеграм-канал компании «Лига безопасного интернета»)*.

Одновременно предоставляются ссылки:

https://okko.tv/serial/na-krjuchke-592260973 *(профилактический российский сериал 204 года «На крючке», который полезно посмотреть даже тем, кто уверен, что никогда не попадется на уловки мошенников)*;

https://www.kinopoisk.ru/film/1316625/ *(корейский фильм «Грязные миллионы» о телефонном мошенничестве)*.

Следственный департамент МВД России

Что такое биометрические данные и в чем их главная угроза?

Биометрические персональные данные – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (отпечатки пальца, геометрия лица, голос и иное).

Угроза кражи биометрических данных – это угроза вашей идентичности, репутации и приватности в долгосрочной перспективе.

В настоящее время мошенники в основном собирают фотографии и голоса россиян.

Как мошенники использую собранные данные:

1. Чтобы создавать дипфейки для обмана близких, друзей и коллег. Мошенники создают правдоподобные легенды и, в конечном итоге, выманивают у жертвы деньги.
2. Кража аккаунтов. Некоторые сервисы требуют подтверждения личности по видео. Получив нужные ракурсы лица, мошенники проходят такие проверки.
3. Фальшивые профили и документы. Фотографии используют для создания поддельных аккаунтов в соцсетях, схем с «Fake boss» (поддельный руководитель) или фиктивных анкет на вакансию.
4. Шантаж и дескридитация. Данные могут попасть в открытый доступ или продаваться на теневых форумах. Это риск репутационных потерь.

Для сбора биометрических данных злоумышленники могут:

- совершать вам звонки по видеосвязи и во время общения вести видеозапись разговора;
- рассылать массовые сообщения, как правило, со ссылкой на фишинговые (поддельные) сервисы, к примеру, якобы «Госуслуги», банковский сервис или интересное приложение, и под предлогом оплаты услуги или составления заявки требовать подтвердить личность: включить камеру и показать лицо со всех ракурсов или, глядя в камеру, помахать рукой;
- собирать ваши фотографии и видео из социальных сетей, где вы выложили их с открытым доступом.

Следует отметить, что запись видео с лицом гражданина не позволяет получить доступ к банковским приложениям и платежным средствам. Российские банковские биометрические сервисы устойчивы к дипфейкам, даже если они сделаны на основе собранных данных по таким сценариям. Недостаточно для успешной идентификации и простой записи голоса.

В то же время в настоящее время уже зафиксировано, что биометрические данные активно используются злоумышленниками как инструмент психологической манипуляции после взаимодействия российских граждан с фишинговым (поддельным) ресурсом.

Пользуясь тем, что данный способ верификации относительно новый, мошенники активно применяют сообщения о взломе или утечке биометрических

данных в схемах, предполагающих инициативный звонок гражданина в поддельную техническую поддержку.

Так, в Республике Башкортостан заявителю после взаимодействия с фишинговым (поддельным) ресурсом поступило уведомление «Вы успешно подтвердили вход с помощью биометрии по фото с нового устройства Айфон 14 Про Макс. Выгрузка данных запущена, по окончанию отчет будет отправлен на почту mamontscam1312@yandex.ru». После чего с ним связался неизвестный и, представившись сотрудником портала «Госуслуги», под предлогом обеспечения безопасности денежных средств, путем обмана похитил 500 000 рублей и 1 200 долларов.

Несмотря на отсутствие фактов применения биометрических данных для неправомерного доступа к платежным сервисам, необходимо соблюдать базовые меры безопасности.

Принципы финансовой самообороны с приходом новых технологий не меняются.

Никто из официальных лиц (банк, госорганы) не будут запрашивать биометрию (видео с лицом и голосом) по телефону или через смс-рассылку. Поскольку процесс сбора биометрии проходит в строго регламентированном порядке. Единственный безопасный способ сдать свои биометрические данные для Единой биометрической системы – это прийти с паспортом в отделение банка, который подключен к системе и пройти процедуру в специальном кабинете.

Одновременно рекомендуется использовать сложные и разные пароли, а также двухфакторную аутентификацию везде, где это возможно.

Также необходимо подозрительно относится к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься»), с темами про финансы, банки, в том числе со ссылками, особенно если они длинные или наоборот, использовались сервисы сокращения ссылок.

Нельзя переходить по ссылкам из письма, если они заменены на слова. Следует проверять ссылки, даже если письмо получено от коллеги или знакомого. Нужно помнить, что их аккаунты и личные кабинеты могли взломать. Также на фишинговом сайте часто есть орфографические ошибки и некорректно работающие элементы.

Что делать, если все же Вы стали жертвой:

- незамедлительно позвонить в банк (не по номеру из смс, а по номеру телефона, указанному на оборотной стороне банковской карты) и заблокировать счета и карты;

- сменить все пароли, которые вводились, особенно если они от онлайн-банков и «Госуслуг»;

- подать заявления в полицию, а также в Роскомнадзор о неправомерной обработке персональных и биометрических данных и хищении/попытке хищения денежных средств.

Главная защита от атак, связанных с биометрией, - это личная бдительность и понимание того, что Ваши уникальные данные нельзя передавать кому бы то ни было удаленно. Любая просьба это сделать – это верный признак мошенничества!

Следственный департамент МВД России

Отвечая на поставленные вопросы можно отметить, что актуальность противодействия мошенникам на рынке недвижимости связана с принятыми банковским сектором мерами по защите денежных средств на счетах клиентов.

Внедрены надежные Антифрод-системы по блокировке вывода денежных средств со счетов клиента. Постоянно расширяется понятие операции без согласия клиента, принимаются отрицательные решения по заявкам на получение кредитов, поскольку сотрудники банка четко считывают клиента, находящегося под воздействием обмана.

Поэтому злоумышленники стали использовать сценарии хищения имущества граждан, исключив участие банков и мошеннические сценарии с квартирами, где жертвы под воздействием злоумышленников продают свое единственное жилье, действительно существуют в российской судебной и социальной практике.

Одновременно жертвы не только продают квартиры, но и машины, закладывают ценное имущество в ломбарды деньги передают криминальным курьерам.

И все это несмотря на то, что в глобальном понимании, на текущий период население и профессиональные участники рынка гораздо больше информированы о наличии ИТ-преступности, способах их совершения и методах противодействия ей, а также правилах безопасного поведения.

Данные сценарии находятся на стыке правовой неграмотности, а также мошенничества и в основном получили распространение в крупных городах и областях: Москва, Санкт-Петербург, Новосибирская, Челябинская, Московская области, где наиболее высокая стоимость жилья.

Случаи продажи пенсионерами квартир, с заведомо ложным утверждением, что они стали жертвами мошенников, при подготовке материалов не замечены.

При выявлении указанных фактов лица подлежат привлечению к уголовной ответственности в соответствии с законодательством Российской Федерации.

Злоумышленники используют денежные средства, похищенные у жертв в результате мошеннических схем с квартирами, для легализации преступных доходов, а также для финансирования деятельности, направленной на подрыв основ государственного строя и безопасности Российской Федерации.

И жертва невольно втягивается в эту цепочку.

Если же жертва знала и осознавала, что участвует в операциях с преступными доходами, то фактически является соучастником ряда преступлений.

Самые распространенные варианты мошеннических схем с квартирами:

1. «Мошенничество под видом сотрудников банка или госорганов».

Во время звонка или сообщения «от сотрудника безопасности банка» или «Росреестра» Вам сообщают что на квартиру пытаются оформить или уже

оформили незаконную сделку. Чтобы «заблокировать» атаку и «защитить» недвижимость, жертву просят:

- взять кредит под залог квартиры и перевести денежные средства на «безопасный счет» (счет мошенников) или передать курьерам;

- «защитить» квартиру от ареста, либо иных проблем с законом, продав ее;

- предоставить удаленный доступ к компьютеру или установить вирусное программное обеспечение под видом «защитного приложения».

2. Легенда о «генеральной доверенности», оформленной от имени жертвы на «украинского террориста».

Во время звонка или сообщения Вам рассказывают о переводах всех денежных средств, продаже квартиры и «как следствие» о «грозящей» Вам уголовной ответственности за финансирование ВСУ.

Следует помнить, что продать квартиру «по доверенности» мгновенно невозможно.

Для отчуждения недвижимости нужна нотариально удостоверенная сделка и госрегистрация перехода права собственности в Росреестре, которая занимает время, так как проверяются документы.

Для распоряжения счетом доверенность должна быть предъявлена банку. Банки в обязательном порядке проверяют ее подлинность, а многие вообще принимают доверенности, оформленные в самом банке. Ни один «террорист» не может получить доступ к вашим деньгам просто по звонку или чужому слову.

Генеральная доверенность не оформляется тайком. Любая нотариальная доверенность требует личного присутствия доверителя у нотариуса и его подписи. Нельзя, чтобы доверенность на ваше имя оформили без вашего участия или по «приказу сверху». Любые рассказы про то, что «за вас уже оформил доверенность» - юридически бессмысленны и лживы.

3. «Мошенничество под предлогом уточнения данных для доставки посылки» или «под предлогом замены счетчиков».

Ярким примером может стать уголовное дело, когда кибермошенники после того, как она продиктовала присланный ей в смс-сообщении код, убедили 75-летнюю жительницу Приморского края в том, что неустановленными лицами был получен доступ в ее личный кабинет «Госуслуг» и теперь ее квартира находится в залоге у неких злоумышленников, в связи с чем недвижимость нужно срочно продать, иначе она перейдет в собственность третьим лицам.

4. «Мошенничество под предлогом получения персональных данных и денежных средств гражданина».

Злоумышленники используют телефонные звонки, электронную почту и мессенджеры, нередко прикладывая поддельные «документы» из Росреестра», чтобы запугать жертву возможной потерей квартиры.

Их цель – вызвать панику и вынудить человека связаться с «службой поддержки» по указанным номерам.

5. «Мошенничество под предлогом участия в специальной операции по поимке преступников».

Ярким примером может стать уголовное дело, когда аферисты, представившись «силовиками», убедили 78-летнюю женщину, что ее телефон «прослушивают» преступники, и для их поимки нужно выполнять их указания «в рамках операции».

Москвичка последовательно положила 1,1 млн рублей из дома в указанное мошенниками места, а также продала 4 квартиры, отдав деньги «посыльным», запланировала оформить ренту на подмосковную квартиру, но вовремя спохватилась. Общий ущерб превысил 50 млн рублей.

Что же происходит после того, как жертва социального инженера продала квартиру и отдала деньги мошенникам?

После того как жертва отдала деньги и оправилась от воздействия социального инженера, она пытается вернуть право собственности.

Справочно: К примеру анализируя полученные данные из 10 территориальных подразделений нами установлено, что после реализации 251 квартиры подано 98 исков в суд, из которых 9 не приняты в связи с ненадлежащим составлением искового заявления, из 89 исков 55 не рассмотрены судами, по 20 право собственности оставлено за покупателями, по 14 – за продавцами.

Практика гражданских судов здесь идет по трем направлениям:

- в суде сделка признается недействительной и покупатель квартиры, являющийся добросовестным, остается и без денег и без квартиры (или 41% таких решений);

- в суде сделка признается недействительной и применяется двусторонняя реституция, право собственности возвращается продавцу с одновременным возложением на него обязанности по возврату денежных средств покупателю (или 39%);

- в суде в исковых требованиях истцу отказывают, жертва сама несет ответственность за свои действия (или 20%).

Во всех исследуемых нами случаях покупатель вводился в заблуждение продавцом, поскольку это часть сценария обмана.

В связи с чем встает закономерный вопрос: «Должен ли покупатель, которым приняты все меры для выяснения воли продавца, отвечать за действия продавца, находящегося под воздействием обмана?».

Сразу стоит оговориться, что не существует официальной статистики, которая бы отслеживала именно «минимальную или наиболее крупную сумму» по квартирам, проданным под воздействием мошенников.

Если говорить о «средней сумме», которую теряет жертва, то она колеблется в широких пределах, но усредненный диапазон можно обозначить как от 1,5 до 6 миллионов рублей. Почему такой разброс? Региональная разница в стоимости жилья. Это главный фактор.

В г. Москве и Московской области ущерб от одной такой сделки может составлять 10-25 млн рублей и более. Квартира в спальном районе г. Москвы легко стоит 12-15 млн. рублей.

В крупных городах-миллионниках (Санкт-Петербург, Екатеринбург, Новосибирск и другие) средний ущерб будет в диапазоне 4-8 млн рублей. В регионах сумма может быть значительно ниже – 1,5-3 млн рублей за стандартную однокомнатную или двухкомнатную в областном центре.

Как защититься жертвам мошенничеств и добросовестным покупателям?

Защититься от таких мошенников можно, выработав «цифровой иммунитет» - набор четких правил и привычек, которые не позволят злоумышленникам Вас обмануть.

Рекомендации для пенсионеров и их родственников.

Самой современной и эффективной стратегией кибербезопасности в эпоху искусственного интеллекта и дипфейков является **принцип нулевого доверия.** Если говорить коротко, его суть можно выразить одной фразой **«Никогда не доверяй, всегда проверяй».**

Главные правила остаются все те же:

1. Получив неожиданную просьбу или указание передать незнакомому лицу деньги, оформить юридическую сделку с квартирой, тем более в ходе телефонного разговора, необходимо на 100% понимать, что это уловки мошенников, и положить трубку. Любая угроза «срочно спасать имущество» - манипуляция.

2. Не действовать в одиночку. Любая крупная сделка должна проходить с участием близких, доверенных родственников или независимого адвоката.

3. Не подписывать документы под давлением. Если вас торопят – это стоп-сигнал.

4. Никаких дистанционных сделок «под ключ». Продажа квартиры – это серьезная юридическая и финансовая операция. Ее нельзя совершить по телефону, через мессенджер или по электронной почте без личных встреч и проверки документов.

5. Росреестр никогда не направляет смс-сообщения в мессенджерах или письма с предложением перейти по ссылке или перезвонить. Официальная переписка ведется исключительно с адресов в домене @rosreestr.ru.

6. Защитите личные данные в цифровом пространстве. Зайдите в личный кабинет на «Госуслугах» и отключите возможность подачи заявлений на регистрацию сделок, если Вы не планируете продажу. Используйте для входа не смс-пароль, а двухфакторную аутентификацию

7. Проверяйте риелторов и компании. Отзывы, лицензии, срок работы на рынке.

8. Используйте услуги нотариуса. Хотя это стоит денег, нотариус обязан проверить дееспособность сторон и законность сделки, что является дополнительной защитой.

«Красные флаги» - при которых нужно бежать от сделки:

1. Продавец избегает личных встреч.

2. Цена значительно ниже рыночной, так как «срочный выгодный вариант» - почти всегда ловушка.

3. Сделка оформляется по доверенности, особенно выданной в другом регионе. Требуйте личного присутствия собственника.

Рекомендации для добросовестного покупателя:

1. Проверяйте продавца. Требуйте личной встречи в продаваемой квартире, в том числе поговорите с ним на отвлеченные темы.

2. Используйте услуги нотариуса, риелтора, а также банковские продукты (аккредитив или эскроу-счет, когда деньги хранятся в банке до момента регистрации перехода права в Росреестре).

3. При этом необходимо помнить, что простые разговоры с лицом, возможно находящимся под воздействием кибермошенников в момент совершения сделки, не помогают.

Решением проблемы станет видеозапись разговора с продавцом квартиры и его роспись в бланках с ответами на вопросы о намерениях продать квартиру,

причинах ее продажи с одновременным предупреждением о последствиях сделки. А это освобождение квартиры и лишение права собственности на нее.

Продавца рекомендуется несколько раз устно и под роспись предупредить, что если ему говорят о том, что квартиру надо реализовать в ходе специальной операции правоохранительных органов, то необходимо сообщить об этом сейчас, что таких операций не бывает. А если продавец скрывает воздействие на него мошенников, то в дальнейшем самостоятельно будет нести ответственность за последствия, наступившие по сделке купли-продажи.

Данные документы станут гарантом добросовестности со стороны риелтора и покупателя и не смогут быть не оценены в суде.

Всегда помните, что сделка с квартирой состоит из 8 ключевых шагов:

1 шаг. Начало: для покупателя – поиск объекта (оценка своих финансовых возможностей, если нужно – предварительное одобрение ипотеки, поиск подходящего варианта), для продавца – публикация объявления (определение рыночной цены, проверка всех документов на квартиру: свежая выписка из ЕГРН, отсутствие обременений, законность перепланировок).

Опции: определение критериев срочности, решение о привлечении риелтора, подготовка и изучение ключевых условий (цена, сроки, мебель, порядок расчета, фотографии объекта).

2 шаг. Первый контакт: для покупателя и для продавца – переписка и обсуждение.

Опции: стороны уточняют детали, а именно проходят опросники здесь и далее: уточняют причины продажи, сроки, порядок расчета, единственное жилье или нет, а также планируемые дальнейшие шаги, к примеру место жительства продавца после сделки.

3 шаг. Знакомство с объектом: для покупателя и для продавца – осмотр.

Опции (или общие действия): проводится личный или дистанционный осмотр квартиры, который фиксируется на видео. На этом этапе также осуществляется прохождение опросников, допускаются к участию свидетели или доверенные лица.

4 шаг. Переговоры: для покупателя и для продавца – торг и предварительные расчеты.

Опции: стороны согласовывают окончательную цену (возможен дисконт) и условия будущей сделки, обсуждается возможность внесения обеспечительного платежа (задатка).

5 шаг. Юридическая и практическая подготовка. Для покупателя и для продавца – подготовка к сделке.

Опции: проводится углубленная проверка документов и чистоты сделки, оценка дееспособности сторон, опрос соседей и родственников, освидетельствование, приобщаются справки из диспансеров, снятие с регистрационного учета всех проживающих и вывоз вещей.

6 шаг. Основное действие: для покупателя и для продавца – сделка.

Опции: нотариальное удостоверение, видеозапись сделки, свидетели, доверенные лица, прохождение опросников, освидетельствование, дополнительные услуги.

7 шаг. Взаиморасчеты: для покупателя – передача денег, для продавца – получение денег.

Опции: выбор безопасного способа расчета (банковская ячейка, аккредитив, счет эскроу), сам расчет, подписание акта приема-передачи квартиры.

8 шаг. Завершение: для покупателя – заезд, для продавца – выезд.

Опции: фиксируются факт выезда/невыезда, действия сторон.

Совмещение практического плана сделки с юридическими и техническими деталями дает полную картину процесса. Это поможет понять, какие важные действия скрываются за каждым, казалось бы, простым шагом.

Следственный департамент МВД России

Информационно-справочные материалы по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Когда мы говорим о глобальном явлении киберпреступности, то такого понятия, как «рекордная сумма» не существует, потому что это не один случай, а миллионы инцидентов и ключевым аспектом является именно совокупный годовой ущерб и средние показатели, которые складываются из множества факторов.

Таким образом, анализируя киберпреступность в России, мы должны смотреть не на мифический «рекорд», а на динамику трех показателей:

- совокупный годовой ущерб;
- количество зарегистрированных преступлений;
- среднюю сумму ущерба на преступление.

Отвечая на поставленные вопросы можно отметить, что киберпреступления распространены во всех без исключения странах. И в каждой стране растет их количество и суммы причиненного ущерба.

Так, в 2024 году Международной группа исследований под руководством Оксфордского университета (Великобритания) определены страны, имеющие самый высокий индекс кибепреступности, такие как: Украина (36,4), Китай (27,86), США (25,01), Нигерия (21,8), Румыния (14,83), Северная Корея (10,61), Великобритания (9,01), Бразилия (8,03), Индия (6,13).

Из-за тотальной цифровизации во всех аспектах жизни, таких как финансы, бизнес, госуправление, по данным Group-IB, общий ущерб от киберпреступлений в мире исчисляется триллионами долларов ежегодно и продолжает расти двузначными процентами в год.

В России суммы похищенных денежных средств также растут. В **2022 году - 91 млрд**, в **2023 году – 156 млрд**, в **2024 году – более 192 млрд** рублей, за **10 месяцев 2025 года** – 158, 6 млрд рублей (в аналогичном периоде прошлого года - 150 млрд). То есть за **три года** население и государство лишилось **не менее 387 млрд** рублей.

Вместе с тем, принимаемые в текущем году правоохранительными органами и банковским сектором правовые и технологические меры позволили добиться определенной положительной динамики. **Прирост киберпреступлений в России сократился[1], что может позволить абсолютному ущербу расти более медленными темпами, чем ранее.**

При этом рост или падение в России «средней суммы» ущерба[2], ***сам по себе не говорит об успехе или провале борьбы с киберпреступностью.***

---

[1] По итогам 10 месяцев 2025 года зафиксировано снижение на 9,5% количества регистрируемых преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий.

[2] В случаях мошенничеств с помощью СМС или звонков от «служб безопасности банка», фиктивных выигрышей «средняя сумма» ущерба с жертвы составляет от 1 000 рублей до 100 000 рублей, при несанкционированных списаниях с банковского счета – несколько тысяч на операцию,

Нелепость и абсурдность сценариев это не признак глупости мошенников, а их тактическое оружие.

Не нужно искать в их методах сложной магии или гипноза. Вся их сила – в эксплуатации простых, примитивных, но безотказно работающих кнопок в нашей психике.

Поэтому сценарии, используемые мошенниками, позволяют вводить в заблуждение даже тех, кто по роду своей деятельности прекрасно осведомлен о происках аферистов. Это и молодежь, которая хорошо ориентируется в интернет-пространстве, и даже руководители, государственные служащие учреждений и организаций, работники банков и операторов связи, которые в свою очередь более осведомлены о способах мошенничества.

Значительную роль здесь играет низкая финансовая и цифровая грамотность населения. Кроме того в периоды кризисов и неопределенности люди становятся более тревожными и подверженными панике, чем активно пользуются злоумышленники.

Таким образом, самой современной и эффективной стратегией кибербезопасности в эпоху искусственного интеллекта и дипфейков является принцип нулевого доверия. Если говорить коротко, его суть можно выразить одной фразой «Никогда не доверяй, всегда проверяй».

Это полная противоположность устаревшему подходу «Доверяй, но проверяй», который и послужил причиной совершения злоумышленниками в 2024 и 2025 годах **2-х *крупных дистанционных хищений,*** *а именно:*

1. В 2025 году у жительницы одного из крупных областных центров России похищены денежные средства в особо крупном размере. Общая сумма ущерба составила свыше 400 млн рублей (в рублях, долларах и евро), что можно назвать «рекордной» суммой.

Злоумышленники, выдававшие себя за сотрудников силовых ведомств, тщательно готовились к преступлению: собирали о жертве информацию из открытых источников, убедили ее участвовать в спецоперации по поимке опасных преступников в качестве «приманки». Для правдоподобности они приобрели дорогие костюмы, арендовали автомобили и частный дом, привлекли курьеров и использовали документы, содержащие недостоверные сведения о личности.

По данному факту к уголовной ответственности ***в составе преступного сообщества*** привлекаются более 5 лиц, в отношении которых избраны меры пресечений в виде заключения под стражу. В ходе следствия у обвиняемых изъято более 7 млн рублей, 40 тыс. долларов и 35 тыс. евро, на указанные ценности наложены аресты.

2. В 2024 году телефонные злоумышленники обманом лишили квартиры известную народную артистку России, причинив имущественный ущерб в особо крупном размере более 200 млн рублей.

В обоих случаях, которые в настоящее время кажутся со стороны нелепыми, поскольку мошенники использовали примитивные сценарии, денежные средства жертвы передавали так называемым «курьерам» для их дальнейшего перевода на «безопасный счет».

Название более детальной информации и конкретных сумм ущерба в интересах потерпевших полагаем некорректным, поскольку это может нарушать их право на конфиденциальность и защиту личных данных.

Несмотря на многообразие мошеннических схем, базовые принципы финансовой самообороны неизменны.

Подводя итог, главные правила остаются все те же:

1. Получив неожиданную просьбу или указание перевести или передать незнакомому лицу деньги, тем более в ходе телефонного разговора, необходимо на 100% понимать, что это уловки мошенников, и положить трубку.

2. Настоящие сотрудники банков или государственных органов никогда не будут запрашивать по телефону или в смс данные ваших карт, пароли или коды подтверждения.

3. Для проверки информации перезвоните в банк или правоохранительные по официальным номерам с их сайтов.

В случае, если гражданин своевременно обращается с заявлением о совершении хищения дистанционным способом, сотрудники органов внутренних дел совместно с банками вовремя реагируют и становится гораздо больше шансов арестовать счета злоумышленников.

Кроме того, Президентом Российской Федерации подписан Федеральный закон, который ***наделил следователей и дознавателей правом без судебного решения приостанавливать расходные операции с денежными средствами, находящимися на счетах,*** использовавшихся в преступной деятельности. Указанная норма вступила в законную силу ***с 1 сентября текущего года.***

Следственный департамент МВД России

Отвечая на поставленные вопросы можно отметить, что нелепость и абсурдность сценариев и способов упаковки денежных средств для последующей их передаче курьерам – это не признак глупости мошенников, а их тактическое оружие и изощренный психологический инструмент.

Не нужно также искать в их методах сложной магии или гипноза. Вся их сила – в эксплуатации простых, примитивных, но безотказно работающих кнопок в нашей психике.

Мошенники через телефон диктуют жертве, во что именно нужно завернуть деньги. Цель – сделать сверток максимально незаметным для посторонних глаз и похожим на обычный предмет, а также психологически обосновать необходимость упаковки.

Рациональный человек в спокойной обстановке сразу заметит нестыковки. Задача мошенника – вывести жертву из состояния рациональности.

Именно абсурдные инструкции по упаковке денег для курьеров решают для злоумышленников несколько задач одновременно:

1. Тест на лояльность и подавление критического мышления, в ходе которого просьба мошенника завернуть деньги в фольгу и положить, к примеру, в банку с крупой, действует на жертву как «ритуал инициации», в ходе которого происходит отсев «неготовых», а именно:

- если жертва начинает спорить, задавать вопросы: «А зачем это?», она демонстрирует, что еще сохранила критическое мышление. Такая жертва для мошенника – рискованный «клиент», который может одуматься в любой момент и тогда злоумышленник либо бросает трубку, либо удваивает давление;

- тот, кто безропотно выполняет абсурдные приказы, уже прошел важнейший тест на внушаемость и психологически готов поверить в последующие, еще более невероятные инструкции.

2. Создание искусственного дефицита времени и когнитивной перегрузки.

Пока жертва ищет дома судорожно фольгу, скотч, коробку из-под сока или иное, чтобы завернуть деньги, у нее не остается ресурсов на главный вопрос: «А кто этот человек и зачем я вообще ему передаю все свои сбережения?». Мозг занят выполнением конкретной, хотя и странной задачи. Это отлично отвлекает от анализа ситуации в целом.

3. Усиление авторитета «специалиста». Мошенник, представляясь сотрудником правоохранительных органов, ФСБ или экстрасенсом создает образ человека, владеющего тайными знаниями. Жертва думает: «Я в этом не разбираюсь, но специалист знает, что делает».

Таким образом, просьба завернуть миллионы в памперс и оставить их в мусорном баке – это не бред сумасшедшего. Это хитросплетенная тактика, направленная на:

- «сегрегацию аудитории» (оставить в «воронке обмана» только самых внушаемых);

- эскалацию вовлеченности (заставить жертву эмоционально и физически «инвестироваться» в процесс обмана).

Значительную роль здесь играет низкая финансовая и цифровая грамотность населения. Кроме того в периоды кризисов и неопределенности люди становятся более тревожными и подверженными панике, чем активно пользуются злоумышленники.

Самые распространенные виды упаковки:

- конверты, газеты и журналы (классический и самый частый вариант. Газетный лист и иное – под рукой, их не жалко, а сверток выглядит как макулатура;

- фольга (мошенники могут объяснять это необходимостью «защиты от электромагнитного облучения» или «блокировкой сигнала»);

- политэтиленовые пакеты (часто в нескольких слоев и как правило черного или зеленого цвета). Просто, доступно и защищает от влаги. Может комбинироваться с бумагой или фольгой;

- газетная бумага в сочетании со скотчем. Чтобы сверток не развернулся, его обильно обматывают скотчем, что делает его похожим на «невзрачный» груз.

Самые нелепые случаи «заворачивания» денежных средств в 2025 году:

- в г. Москве помимо полиэтиленовых пакетов и газет жертвы заворачивали и передавали денежные средства в джинсах и коробках из-под таблеток,

- Республике Северная Осетия – Алания, в г.г. Санкт-Петербурге и Челябинске – в куртках, одеялах, шерстяных костюмах, халатах и носках;

- Забайкальском крае – в полотенцах;

- Алтайском крае, Кемеровской области – Кузбассе и Новосибирской области – в сумках с одеждой и банками с вареньем, помидорами и огурцами, черной ткани.

Понимая, что каждая нелепая деталь в сценарии мошенников – это продуманный психологический удар, становится проще распознать атаку и прервать ее на самом начале, просто положив трубку.

Таким образом, самой современной и эффективной стратегией кибербезопасности в эпоху искусственного интеллекта и дипфейков является принцип нулевого доверия. Если говорить коротко, его суть можно выразить одной фразой «Никогда не доверяй, всегда проверяй».

***Подводя итог,* главные правила остаются все те же:**

1. Получив неожиданную просьбу или указание передать незнакомому лицу деньги, тем более в ходе телефонного разговора, необходимо на 100% понимать, что это уловки мошенников, и положить трубку.

2. Настоящие сотрудники банков или государственных органов никогда не будут просить по телефону или в смс завернуть денежные средства в какую-либо упаковку и передать их неизвестному курьеру.

3. Для проверки информации перезвоните в банк или правоохранительные по официальным номерам с их сайтов.

Следственный департамент МВД России

Отвечая на поставленные вопросы следует отметить, что рост цен на услуги дропов – это практически неизбежный сценарий, основанный на резком увеличении рисков для всех участников преступной схемы из-за принятых в 2025 году правоохранительными органами и банковским сектором действенных мер для блокировки вывода похищенных денежных средств со счетов клиентов.

Совершению отмеченного вида противоправной деятельности способствует вовлечение в преступную цепочку держателей ЭСП, открывающих платежные карты, электронные кошельки и счета на свое имя с целью их дальнейшей передачи или предоставления доступа к ним за денежное вознаграждение третьим лицам, либо для неправомерного осуществления операции по приему, переводу денежных средств, выдаче и (или) получению наличных денежных средств (далее – дропы).

Дропы являются низшим звеном всей цепочки организованной преступной группы, однако без их участия совершение таких преступлений просто невозможно, так как серый рынок сбыта ЭСП и доступа к ним позволяет злоумышленникам выводить похищенные у граждан денежные средства.

В ходе расследования киберпреступлений сотрудниками органов внутренних дел изымается значительное количество электронных средств платежа, которые передавались их держателями иному лицу.

Организаторы мошеннических схем действуют в условиях повышенной конспирации. Ими организовываются и на постоянной основе проводятся инструктажи для дропов, размещаются в информационно-телекоммуникационной сети «Интернет» пособия о том, как вести себя в случае задержания сотрудниками правоохранительных органов. Так называемое «бронирование дропов» осуществляется посредством мессенджеров, в том числе принадлежащих запрещенной в Российской Федерации корпорации «Meta», в условиях отсутствия личного контакта.

Возможность легкого заработка побуждают привлекаемых к противоправной деятельности держателей ЭСП, а также иных лиц, использующих их для обналичивания денежных средств, к совершению аналогичных действий в дальнейшем.

К примеру, многие подростки осознают, что стали частью преступной схемы, но сойти с кривой дорожки не могут — настолько их привлекают легкие деньги или они стали заложниками шантажа преступников. Вот только заканчиваются эти истории печально. Наравне с другими участниками группы несовершеннолетние несут ответственность, становятся фигурантами уголовных дел.

Так, в Алтайском крае, и в г. Омске подростки привлечены к уголовной ответственности за совершение действий по передаче банковской карты и осуществлению операций по переводу похищенных денежных средств.

В г. Казани Республики Татарстан в одном из колледжей большинство учащихся были вовлечены в «дроперство».

Справочно: Государственное автономное профессиональное образовательное учреждение «Казанский энергетический колледж». Сотрудником Следственного департамента МВД России с участием преподавателей и студентов проведена лекция, на которой освещены негативные последствия участия в преступной деятельности по обналичиванию денежных средств. Соответствующая профилактическая информация была размещена в помещениях колледжа.

В зависимости от банка, платежной системы и иных аспектов стоимость услуг дропа варьируется от 1000 до 5000 рублей, а средние сроки использования оформленных на них различных электронных средств платежа составляют от 2 до 15 дней.

Сокрытие преступлений, вывод наличных денежных средств, легализация преступных доходов без действий дропа невозможны, в связи с чем такой вид деятельности является общественно опасным.

Наша задача – разорвать эту цепочку, действуя на опережение и перекрывая каналы мошенничества.

В настоящее время для противодействия данной деятельности между Банком России и МВД России организован информационный обмен. ***Банкам представлено право при выявлении операции без согласия клиента блокировать дистанционное банковское обслуживание счета, на который поступили похищенные денежные средства, а также иных счетов данного лица.***

Кроме того, Президентом Российской Федерации подписан Федеральный закон, который ***наделил следователей и дознавателей правом без судебного решения приостанавливать расходные операции с денежными средствами, находящимися на счетах,*** использовавшихся в преступной деятельности. Указанная норма вступила в законную силу ***с 1 сентября текущего года.***

Справочно: по сведениям Банка России в настоящее время более 18 тысяч (18521) фигурантов окрашены кредитными организациями как участники теневого оборота денег от онлайн-казино, букмекерских контор, криптообменников и других потенциально опасных источников.

Ранее фактором, препятствующим противодействию такой деятельности, являлось отсутствие правового барьера, предусматривающего ответственность за передачу ЭСП, его использование для неправомерного осуществления банковских операций, в том числе по получению денежных средств в наличной форме и даче распоряжения на их последующий перевод.

Сейчас необходимо принять во внимание, что **в *целях ликвидации «каналов вывода» похищенных денежных средств с использованием так называемых «дропов»,*** *передающих злоумышленникам за денежное вознаграждение свои банковские карты и счета,* ***Президентом Российской Федерации подписан Федеральный закон от 24 июня 2025 г. № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации», которым введена уголовная ответственность для «дропов» (указанным Федеральным законом установлен прямой запрет на передачу своих платежных данных злоумышленникам и участие в операциях с похищенными средствами[1]).***

---

[1] Вступил в законную силу с 5 июля 2025 года.

Справочно: в настоящее время внимание МВД России сконцентрировано в том числе и на тех дропах, установленных по уголовным делам, возбужденных с 5 июля текущего года. Именно их деятельность будет подлежать процессуальной оценке.

В г.г. Москве, Калуге, Оренбурге, Курске, Ульяновске уголовные дела в отношении дропов уже направлены в суд, а в г.г. Москве и Ульяновске к ним уже применены наказания по решениям судов.

Государство активно принимает меры, но прямого термина «статистика дропперства» в МВД России нет.

Лучший индикатор – это статистические отчеты МВД России «Состояние преступности» (количество зарегистрированных преступлений) и «Сведения о материальном ущербе от преступлений, совершенных с использованием информационно-телекоммуникационных технологий».

Принимаемые правовые и технологические меры позволили добиться определенной положительной динамики. **Прирост киберпреступлений сократился.**

Если в 2024 году динамика прироста составляла 13%, то по итогам 10 месяцев 2025 года зафиксировано снижение на 9,5% количества регистрируемых преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий. При этом количество преступлений, предусмотренных ст. 158 («Кража») УК РФ снизилось на 21,8%, ст. 159 («Мошенничество») УК РФ - на 7,4%.

Данная статистика является прямым следствием превентивных мер банков и правоохранительных органов, которые, эффективно блокируя операции по переводам денежных средств на ранних стадиях, вынуждают преступные группы к активному привлечению курьеров.

В результате, только за прошедший месяц задержано 86 криминальных курьеров, предотвращены мошенничества в отношении 827 граждан, сумма предотвращенного ущерба составила 300 млн рублей.

Киберпреступления распространены во всех без исключения странах. И в каждой стране растет их количество и суммы причиненного ущерба.

Так, в 2024 году Международной группа исследований под руководством Оксфордского университета (Великобритания) определены страны, имеющие самый высокий индекс кибепреступности, такие как: Украина (36,4), Китай (27,86), США (25,01), Нигерия (21,8), Румыния (14,83), Северная Корея (10,61), Великобритания (9,01), Бразилия (8,03), Индия (6,13).

Из-за тотальной цифровизации во всех аспектах жизни, таких как финансы, бизнес, госуправление, по данным Group-IB, общий ущерб от киберпреступлений в мире исчисляется триллионами долларов ежегодно и продолжает расти двузначными процентами в год.

Несмотря на снижение количества регистрируемых IT-преступлений, в России суммы похищенных денежных средств также растут. В **2022 году - 91 млрд**, в **2023 году – 156 млрд**, в **2024 году – более 192 млрд** рублей, за **10 месяцев 2025 года** – 158, 6 млрд рублей (в аналогичном периоде прошлого года - 150 млрд). То есть за **три года** население и государство лишилось **не менее 387 млрд** рублей.

Одновременно, согласно сведениям Банка России в 2023 году объем операций без согласия клиентов увеличился по сравнению с 2022 годом

на 11,48 % и составил 1 165 990 на общую сумму 15 791,414 млн рублей. На социальную инженерию пришлось более 50% инцидентов, при этом доля возмещенных (возвращенных) средств не превысила 4%.

В 2024 году объем операций без добровольного согласия клиентов увеличился по сравнению с 2023 годом на 74,36% и составил 1 197 440 на общую сумму 27 534,31 млн рублей.

Вместе с тем, следует отметить, что качественная обработка каналов вывода похищенных денежных средств, принятие закона об уголовной ответственности дропов, пресечение преступной деятельности курьеров, блокировка банками управления счетами **позволили сократить прирост ущерба.**

Темпы роста за январь-июнь снизились с +31,0% до +5,6% в январе-октябре. За 4 месяца действия правовых барьеров сумма причиненного ущерба снизилась на 18% (с 75 млрд в июле-октябре 2024 г. до 61,6 млрд в тот же период текущего года).

Установилась позитивная динамика с ежемесячного сокращения по сравнению с АППГ суммы ущерба: в сентябре – на 17,4%, в октябре уже на 31,6%.

Подводя итог обращаем внимание, что значительную роль играет финансовая, правовая и цифровая грамотность населения, а именно:

- если на ваше имя оформлены банковские карты, которые переданы знакомым или за денежное вознаграждение иным лицам, и ими воспользуются мошенники, доступ к управлению всеми вашими счетами будет заблокирован, вы попадете так скажем в «черный» список банков и восстановить управление счетами не так просто.

Поэтому примите самостоятельно меры к блокировке карт, которые утеряны или переданы в пользование третьим лицам;

- если вы участвовали в проведении операций по обналичиванию похищенных денежных средств, либо передали свою банковскую карту третьему лицу, необходимо обратится в полицию.

Обращаем внимание, что в пункте 4 примечаний к статье 187 УК РФ введено специальное основание для освобождения от уголовной ответственности.

Так, в случае, если лицо, являющееся клиентом оператора по переводу денежных средств, впервые совершило преступление, предусмотренное частями третьей и четвертой статьи 187 УК РФ добровольно сообщило об этом в орган, имеющий право возбудить уголовное дело, и (или) активно способствовало раскрытию и (или) расследованию преступления, оно освобождается от уголовной ответственности за его совершение.

Следственный департамент МВД России

Информационно-справочные материалы по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Официальная статистика МД России по обращениям о мошенничествах в разрезе праздничных периодов отдельно не ведется. Однако существует такое понятие, как «четкая закономерность» - когда спрос рождает предложение.

В преддверии праздников и распродаж люди массово ищут выгоду, активно покупают подарки, билеты на культурные мероприятия и следят за акциями.

Злоумышленники этим активно пользуются, так как психологическая готовность человека к выгодной покупке значительно снижает его бдительность.

Какие именно схемы обмана становятся самыми популярными у злоумышленников?

Фишинг – это одна из ключевых угроз, но не единственная. Что именно делают злоумышленники, подстраивая свои схемы под потребительские тренды:

- резко наращивают объемы фишинговых рассылок с фейковыми акциями и ссылками на сайты-клоны;

- создают поддельный страницы популярных маркетплейсов, в том числе осуществляющих реализацию билетов, предлагая «неслыханные» скидки;

- активнее используют схемы с предзаказом дефицитных товаров, играя на ажиотаже.

Таким образом, среди ***основных «трендов» мошенничества в сфере продажи билетов, которых стоит опасаться в предверии новогодних праздников и зимних каникул, можно выделить следующие способы:***

1. Создание злоумышленниками сайтов – двойников (копий официальных сайтов известных касс).

Для создания фейковых сайтов-клонов мошенниками используются шаблоны и автоматизированные скрипты, которые позволяют развернуть точную копию легального сайта буквально за несколько часов.

С этой целью регистрируются доменные имена, похожие на имя известного бренда, с различными опечатками. «Жизненный цикл» такого сайта короток – от нескольких часов до 2-3 суток.

Этого времени достаточно, чтобы собрать достаточное количество жертв, после чего мошенники его бросают и запускают новый.

2. Размещение в сети Интернет рекламы несуществующих билетов по «низкой» цене до начала официальной продажи, а также продажа несуществующих или уже использованных бумажных билетов.

3. Продажа копий/скриншотов электронных билетов. Один билет продается десяткам людей. Первый, кто придет на мероприятие, пройдет, остальные останутся у входа.

4. Использование легальных площадок перепродаж (к примеру Авито, Юла), когда злоумышленник после предоплаты блокирует покупателя.

5. Генерация поддельных QR-кодов, которые не будут считываться сканером или ведут на фишинговый сайт при «проверке».

6. Предложение «вернуть» деньги за отмененное мероприятие по фальшивой ссылке.

Что делают власти и организаторы?

1. МВД России и Роскомнадзор блокируют фишинговые сайты.

2. Организаторы и площадки внедряют именные билеты с паспортным контролем.

3. Банки улучшают системы Антифрод для отслеживания подозрительных операций.

4. Легальные площадки создают официальные площадки для безопасной перепродажи по фиксированной цене.

Но осторожность и осведомленность покупателя остаются основными инструментами защиты.

Самой современной и эффективной стратегией кибербезопасности **является принцип нулевого доверия.**

Если говорить коротко, его суть можно выразить одной фразой «Никогда не доверяй, всегда проверяй».

Советы покупателям:

1. Покупайте билеты только у официальных распространителей. Проверяйте список на сайте артиста, организатора или мероприятия. Основные легальные площадки: Кассир.ру, Яндекс.Афиша, Ticketland.ru и др.

2. Верифицируйте сайт. Проверяйте домен (адрес сайта), наличие SSL-сертификата (замочек в строке браузера), юридических данных компании.

3. Остерегайтесь предоплаты переводом на банковскую карту физическому лицу. Используйте безопасные способы оплаты, которые можно оспорить (к примеру, сервисы официальных касс).

4. Тщательно проверяйте продавцов на вторичном рынке, а именно:

- смотрите рейтинг, давность аккаунта, историю других продаж, требуйте оригинал чека из официальной кассы;

- для электронных билетов – договоритесь о встрече у кассы мероприятия для совместной активации или проверьте билет через официальное мобильное приложение кассы (оно сканирует QR и показывает валидность).

5. Не поддавайтесь на уловку мошенника и используемую им технологию психологического давления: «билеты заканчиваются».

6. Подозрительно относитесь к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься», «купи»), с темами про финансы, в том числе со ссылками, особенно если они длинные или наоборот, использовались сервисы сокращения ссылок.

7. Не переходите по ссылкам из письма, если они заменены на слова. Также на фишинговом сайте часто есть орфографические ошибки и некорректно работающие элементы.

Но если все же попались на удочку мошенника, алгоритм действий должен быть таким:

1. Немедленно позвоните в свой банк по номеру с обратной стороны карты и заблокируйте ее, либо сообщите что осуществлена операция без согласия клиента. Блокировку банковской карты можно также осуществить в мобильном приложении банка.

2. Обратитесь с заявлением в полицию.

3. Если вы ввели логины и пароли от каких-либо сервисов, немедленно смените их, а также включите двухфакторную аутентификацию.

Главное – не паниковать, а действовать быстро. Ваши первые действия определяют шансы вернуть денежные средства.

Следственный департамент МВД России