**Доклад на аппаратную учебу.**

**Обзор мошеннических схем 2024 года и методы защиты от них.**

В России IT-преступления составляют 40% от общего числа преступлений, их зарегистрировано около 300 тысяч, что на 13% больше, чем в 2023 году. В Югре зарегистрировано более 14 тысяч таких преступлений, их число оставляет 53% от общего количества зарегистрированных в округе. Ущерб, причиненный гражданам Югры более 3 миллиардов рублей.

Наш район не исключение – в 2024 году произошел рост IT-преступлений на 64% - зарегистрировано 158 ИТТ-преступлений (п.г.96). Расследовано 9 преступлений или 7% от числа зарегистрированных. Совокупный ущерб для граждан района составил почти 45 миллионов рублей (в 2023 – 16 миллионов рублей).

За 3 недели 2025 года в районе совершено 9 ИТТ-преступлений, которыми причинен ущерб 6 гражданам на сумму более 1,5 миллионов рублей (158 УК РФ – 2; 159 УК РФ – 4, 272 УК РФ – 3). Среди наибольших ущербов: в п. Кондинское 175000 рублей и 900000 рублей; в п. Междуреченский – 350000 рублей. Среди потерпевших есть студенты, пенсионеры, люди разных профессий, разного уровня образования, родственники граждан, проходящих службу на СВО). Граждане продолжают доверять мошенникам, сообщают сведения от банковских карт, иную требуемую информацию.

К новым видам ИТТ-преступлений фиксируемых в районе нужно отнести неправомерный доступ к компьютерной информации (предусмотрено ст. 272 УК РФ). В 2024 году в ОМВД России по Кондинскому району зарегистрировано более 100 сообщений граждан о неправомерности доступа к личным кабинетам граждан на сайте «Госуслуги». Неизвестные по телефону представляются сотрудниками пенсионного фонда, налоговой инспекции, представителями страховых компаний, медицинских или образовательных учреждений, мобильными операторами. Под любым предлогом, в интересах граждан, просят сообщить коды в поступающих СМС-сообщениях, которые в последствии используют для входа в личный кабинет «Госуслуг», блокируют доступ для пользователя и, используя возможности сайта, распоряжаются персональными данными гражданина для подачи заявлений на взятие кредитов.

Мошеннические схемы становятся всё более продуманными. Людям сложнее защитить себя от потери, как собственных накоплений, так и кредитных денег. В некоторых случаях можно даже лишиться имущества: например‚ если продать его под давлением и перевести полученную сумму злоумышленникам.

**Приведём примеры, как уберечь себя от мошенничества:**

«Основные каналы — звонки от якобы сотрудников правоохранительных органов, Росфинмониторинга, Банка России, от управляющих компаний». Звонки могут поступать и от имени других государственных организаций либо банков. Всё чаще преступники прибегают к цепочке мошеннических звонков, когда второй звонок — следствие первого. Например, сначала злоумышленники могут позвонить человеку от имени любого ведомства и обмануть, что «мошенники» пытаются украсть деньги с его счетов. Для защиты средств их попросят перевести на «безопасный» счёт. Далее позвонят «из полиции» и предложат принять участие в поимке мошенников в течение последующих разговоров. Задача преступников — убедить человека перевести как можно больше денег, в том числе взять кредит для этого. Причины таких вложений будут обосновывать благими целями: чтобы поймать мошенников. Звонящие будут стараться постоянно оставаться на связи, чтобы не дать человеку остановиться и подумать. «Таким образом, преступники запутывают жертву и пользуются её стрессом».

Иногда мошенники могут совершать видеозвонки в мессенджерах. Преступники представляются сотрудниками государственных служб или банков. При этом на фоне у звонящего могут быть убедительные «декорации»: флаг России, портрет президента, символика банка и так далее. Так они дополнительно уверяют человека в реальности происходящего. Также мошенники могут позвонить по видеозвонку уже после обычного звонка. «Изначально нужно понимать, что представители Росфинмониторинга или Банка России вообще не звонят обычным людям, физлицам: они с ними не работают». По телефону и в мессенджерах с видеозвонком нельзя сообщать никакой информации незнакомым людям, даже если они представляются сотрудниками МВД, прокуратуры, ФСБ. Все показания предоставляются только лично в соответствующих ведомствах. При звонке можно попросить звонящего прислать официальную повестку и повесить трубку. Сотрудники различных госструктур никогда не звонят в мессенджерах и не используют видеосвязь для общения с гражданами. Людям также могут поступать сообщения: как в мессенджерах и социальных сетях, так и в СМС. Обычно в них есть ссылки на мошеннические сайты, где нужно ввести реквизиты карты.

**Например:** Сообщение может быть отправлено якобы от имени какого-нибудь магазина или маркетплейса. Там укажут, что человек выиграл бонус и для его получения нужно перейти по ссылке. Далее система попросит ввести личные данные и банковские реквизиты. Если заполнить все поля, то вместо зачисления бонуса с карты спишутся деньги. В сообщениях мошенники также могут общаться с жертвой и убедить её перевести деньги под любым предлогом, как и при звонке.

**Какие способы мошенничества есть у преступников?**

Сценариев обмана очень много, и мошенники постоянно придумывают новые: предугадать все схемы невозможно. Однако есть одна общая черта: злоумышленники стараются с первых минут разговора вызвать у человека яркий всплеск эмоций и стресс, заставить действовать быстрее, не раздумывая.

**Манипуляция страхом:** Мошенники могут сказать, что человеку угрожает какая-то серьёзная опасность: он может потерять деньги, квартиру, близкого родственника, сесть в тюрьму и так далее. Иногда схема строится на том, что с близким человеком случилось что-то ужасное: мама попала в аварию, ребёнок оказался в больнице. На фоне стресса человек очень уязвим, и может перевести мошенникам все деньги.

**Как этого избежать:** в таких ситуациях нужно сразу класть трубку и связываться с родственниками, чтобы прояснить обстоятельства. Услышав, что с близким человеком всё в порядке, можно быстрее успокоиться и избежать потери денег. Если звонящий представляется сотрудником банка — нужно класть трубку и звонить в поддержку банка. Номер поддержки обычно указан на обороте банковской карты либо на сайте или в приложении банка.

**Долгосрочные схемы:** некоторые мошенники пытаются надёжнее «завербовать» человека путём долгого общения. Например, могут позвонить от имени «следователя» по поводу «тайного дела», о котором нельзя никому говорить. Тогда человека выставляют героем, который должен помочь в раскрытии преступления. Помощь сопровождается переводом средств мошенникам. Из-за того, что человека убеждают молчать и хранить «секрет», он может ничего не рассказывать близким, которые могли бы помочь ему.

**Как этого избежать:** нужно поступать ровно наоборот: поделиться ситуацией с друзьями и родственниками. Самостоятельно пересказав слова мошенников, можно проанализировать схему и понять, что это обман. Также близкие люди приведут аргументы в пользу того, что это злоумышленники.

**Давление из-за политической ситуации:** с учётом политической ситуации и законодательства РФ мошенники могут сказать жертве, что с её счёта перевели деньги какой-нибудь запрещённой в России организации. Боясь уголовного преследования, человек может вывести деньги на якобы «безопасный» счёт.

**Как этого избежать:** в такой ситуации важно сохранять спокойствие. Чтобы убедиться, что переводов в запрещённые организации не было, стоит повесить трубку и проверить ленту операций в приложениях банков. Там не будет указано никаких переводов, если сам владелец счёта их не совершал и никому не давал данные для входа в онлайн-банк.

**Использование реальной информации о человеке:** мошенники также могут следить за социальными сетями жертвы и использовать информацию оттуда. Например, если они увидят пост о смерти близкого человека, то могут позвонить от имени «ритуальных услуг» для оплаты. Люди, переживающие горе, могут хуже анализировать ситуацию и перевести деньги. Как этого избежать: лучше не выкладывать данные о предстоящих делах в сеть. Фотографиями в соцсетях можно поделиться, когда какое-либо мероприятие или поездка уже пройдут и эмоции от них утихнут. Это касается и негативных, и позитивных ситуаций.

**Фиктивные знакомства:** бывает, что людей обманывают с помощью новых знакомств. Например, «девушка» может написать парню, завести с ним романтическое общение и попробовать получить от него деньги. Скажем, предложить перевести их для оплаты билетов на совместное мероприятие. Или прислать фиктивную ссылку на их оплату. Фиктивная форма для оплаты выглядит как официальная, однако в ссылке могут быть опечатки — она может немного отличаться от официальной. Например, там будет указано aficha вместо afisha.

**Как этого избежать:** перед оплатой стоит обратиться в поддержку сервиса, чтобы узнать: принадлежит ссылка их компании или нет. А ещё иногда система безопасности браузера может предупредить пользователя, что форма может быть мошеннической.

**Наиболее популярные схемы мошенничества в 2025 году**

Кроме звонков от якобы сотрудников правоохранительных органов, Росфинмониторинга, Банка России и управляющих компаний, есть и иные популярные сейчас схемы. Взлом «Госуслуг» под предлогом замены счётчиков. В последнее время часто звонят с просьбой о замене счётчиков на воду: «Вам предложат оставить заявку на замену счётчиков: для этого нужно указать пароль, который пришёл в СМС. Если назвать пароль, можно потерять доступ к своему аккаунту на «Госуслугах»: мошенники быстро сменят пароль и контрольный вопрос». Далее мошенники звонят уже от имени «Госуслуг» или Росфинмониторинга по поводу взлома аккаунта. В ходе разговора мошенник выясняет, сколько денег на счетах жертвы, и предлагает перевести их на «безопасный» счёт. Переводить деньги ни в коем случае нельзя. Нужно положить трубку и срочно обратиться в ближайший МФЦ, чтобы исправить ситуацию и получить доступ к аккаунту.

**Использование подставных лиц для оформления счетов:**

Помимо телефонного мошенничества, также актуальна схема с использованием так называемых «дропов» (подставных лиц). Их используют для незаконных операций по банковским счетам — они даже могут не подозревать, в чём участвуют. Будущих дропов мошенники чаще ищут в социальных сетях либо по знакомству. Им предлагают за определённую плату получить на свой счёт деньги и перевести их по нужным реквизитам. Иногда дропа подговаривают сделать нотариальную доверенность, чтобы мошенник смог открыть банковский счёт и распоряжаться им». С весны 2024 года, по данным Росфинмониторинга, наблюдается кратный рост таких случаев. Соглашаться так «подзаработать» категорически нельзя — это стопроцентное мошенничество, которое может грозить уголовной ответственностью.

**Как защитить себя от мошенников:**

Чтобы не стать жертвой мошенников рекомендуем:

Никогда не сообщать никаких паролей, данных банковских карт или паспорта кому-либо: кто бы ни звонил и кем бы ни представлялся. Если в телефонном разговоре человек спрашивает код из СМС или банковские данные, можно смело класть трубку — это мошенник. Росфинмониторинг и Центробанк не имеют права блокировать банковские счета и открывать «безопасные» счета для защиты от мошенников. Они вообще не работают с физическими лицами. Если звонят от имени этих организаций — это точно обман. При звонке «из банка» всегда лучше положить трубку и перезвонить самостоятельно по номеру телефона, указанному на банковской карте или официальном сайте организации. Не стоит вообще отвечать на звонки с незнакомых номеров, в том числе через мессенджеры. Не нужно доверять предложениям о лёгком заработке, внезапном выигрыше и получении бонусов, особенно если для этого нужно вводить данные карт. Следует установить определитель номера, который может отсеивать нежелательные звонки. Это поможет заранее понять, кто звонит, и сэкономить время на ненужные разговоры.

**Что делать, если уже стал жертвой мошенников:** стать жертвой злоумышленников может абсолютно любой человек, вне зависимости от уровня образования, социального положения и других факторов. Нет причин чувствовать себя виноватым, так как вина всегда на преступнике, а не на жертве. Нужно смело обращаться в полицию и писать заявление. Если мошенникам известны реквизиты карт, то нужно сразу их заблокировать — в приложении либо через поддержку банка. Также можно оставить обращение на оспаривание перевода преступникам. Работники банка рассмотрят, можно ли вернуть деньги. Ещё в поддержку можно отправить талон о принятии заявления в полиции — при запросе от органов, банк поможет в раскрытии дела. Если мошенники получили доступ к «Госуслугам», нужно как можно скорее обратиться с паспортом в ближайший МФЦ для смены пароля. Там же можно оформить заявление о замене паспорта, чтобы данные предыдущего стали недействительными и мошенники не могли ими воспользоваться.