МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ОБЩИЕ СВЕДЕНИЯ

Материал подготовлен для родителей учащихся в целях ознакомления с основными схемами злоумышленников, осведомленности об опасностях, к которым могут подвергнутся дети в Интернете, и содержит свод памяток и рекомендаций от представителей Управления по борьбе с киберпреступностью МВД России и АНО «Диалог Регионы».

ОСНОВНЫЕ ПОНЯТИЯ

Дропперы/дропы (от англ. drop — «бросать», «уронить») — люди, которые задействованы в нелегальных схемах по выводу средств с банковских карт через свои счета и карты. Люди, в том числе и несовершеннолетние лица, нередко становятся дропперами, даже не подозревая об этом (что не освобождает их от ответственности за необдуманный шаг).

Дропперство (Дроппинг) — тем, чем занимаются дропперы.

Кибербезопасность — защита личной информации имеет критическое значение, поскольку в цифровом пространстве данные становятся ценным активом. Персональные сведения, такие как пароли, номера банковских карт или домашний адрес, могут стать целью злоумышленников для кражи средств или использования личных данных в корыстных целях.

Соблюдение правил цифровой гигиены — использование сложных паролей, двухфакторной аутентификации и осторожность при переходе по подозрительным ссылкам — помогает сохранить приватность и обезопасить свою цифровую жизнь от взломов и мошенничества.

Среди основных угроз в интернете выделяются следующие:

Фишинг (англ. phishing от **fishing** «рыбная ловля, выуживание») — вид интернет-мошенничества, с помощью которого злоумышленники получают доступ к конфиденциальным данным пользователей (реквизиты банковских карт, логины и пароли аккаунтов), а также обманом предлагают загрузить вредоносные программы или продают несуществующие услуги.

Фишинговые сайты — это, простыми словами, поддельные сайты известных компаний, например, банков, социальных сетей, маркетплейсов, госорганов. Они могут походить на оригиналы интерфейсом, однако у них искаженное доменное имя.

Жертвы злоумышленников «попадают на крючок» — людиих посещают, переходя из сообщений в мессенджерах, социальных сетях или фишинг-писем на электронной почте, где им предлагают срочно перейти по ссылке, под каким-либо увлекательным предлогом.

Интернет-мошенничество — может проявляться в различных схемах обмана с целью кражи денег.

Компьютерные вирусы и вредоносное программное обеспечение — способны повредить файлы, ограничить доступ к мобильному устройству или компьютеру, тайно собирать данные о действиях пользователя.

Сваттинг (от англ. SWAT, swatting, «вызов спецназа») — заведомо ложное сообщение об угрозе преступления или о происшествии. Делается это для того, чтобы привлечь внимание экстренных служб или правоохранительных органов и направить сотрудников служб по ложному адресу.

Доксинг (англ. doxing, от сокр. docs — документы) — это сбор и распространение личной информации о человеке без его согласия. Эти действия не всегда незаконны, но являются нарушением сетевого этикета и часто запрещены внутренними правилами интернет-сообществ. Причиной доксинга может являться желание шантажировать жертву, отомстить ей или затравить её. Также термин употребляется в отношении сбора чувствительной информации об организациях.

Кардинг (от англ. carding) — вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов. Мошенники кроме звонков напрямую могут находить реквизиты платежных карт на взломанных серверах интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров.

ПОЛЕЗНЫЕ ССЫЛКИ

Дроперы	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Основные этапы мошеннических схем	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Родительский контроль	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Вербовка детей	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Вовлечение в преступную деятельность	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Вымогательство	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Кибербуллинг	https://disk.yandex.ru/d/gzXjRZ-efvFRdg
Запись методического семинара для педагогов по подготовке и проведению 2 марта 2026 года внеурочного занятия «Разговоры о важном»	https://disk.yandex.ru/i/nkJ-rUMZbeIl2w

ДРОППЕРСТВО И АРЕНДА АККАУНТОВ

Статистические сведения

В 2025 году количество зарегистрированных преступлений в сфере противоправного использования информационно-коммуникационных технологий составило 627 тысяч, из которых 65% пришлось на преступления мошеннического характера (против собственности) (430,9 тыс.).

Посягательства в этой сфере зачастую совершались в отношении несовершеннолетних. В 2025 году выявлено более 4,5 тыс. преступлений, связанных с неправомерным оборотом средств платежей, количество несовершеннолетних, привлеченных к уголовной ответственности за данные преступления, с 2023 года возросло в 17 раз (с 2 до 34).

В базе дропперов, которую ведет Банк России, собраны сведения о порядка 1,2 миллиона граждан, которые в той или иной форме помогали мошенникам в совершении противоправных действий. При этом база продолжает активно пополняться: ежемесячно в российских банках открывается около 100 тысяч счетов, которые впоследствии используются для незаконных целей.

Дропперы — кто это?

Для преступников обман жертвы – только первый шаг. Когда деньги выманили, их нужно вывести со счетов пострадавшего так, чтобы замести следы. Украденные средства проходят через карты подставных лиц, а затем обналичиваются. Таких подставных лиц называют дропперы или дропы.

Люди, в том числе и несовершеннолетние лица, нередко становятся дропперами, даже не подозревая об этом (что не освобождает их от ответственности за необдуманный шаг). Чтобы сделать их соучастниками преступления, злоумышленникам достаточно завладеть банковскими реквизитами.

Когда преступники в очередной раз крадут деньги со счета или убеждают владельца средств перевести их на «безопасный счет», они указывают данные не личных платежных инструментов, а банковских карт дропперов.

Как дети становятся дропперами?

Преступники действуют несколькими способами:

1. Выманивают у доверчивых подростков реквизиты уже оформленной платежной карты. Преступники завладевают ими разными способами. Нередко они находят потенциальных жертв в чатах онлайн-игр и предлагают купить какой-либо игровой предмет или бонус, для чего просят сообщить полные реквизиты банковской карты (включая CVC-код).

2. Размещают на различных ресурсах объявления с вакансиями для несовершеннолетних, предлагая выгодную подработку. Платежные реквизиты они предлагают сообщить под предлогом перечисления будущей зарплаты. Иногда мошенники действуют и путем прямых угроз: например,

сообщают, что при отказе сообщить номер карты, родителям ребенка грозят обвинения в терроризме или финансировании экстремистской деятельности.

3. Просят оформить новую карту или открыть счет, а затем передать реквизиты или пластиковое платежное средство другим лицам за небольшую плату. В такой ситуации злоумышленники нередко представляются банковскими менеджерами. Они убеждают детей, что должны выполнить план продаж определенных продуктов и получить премию, частью которой готовы поделиться. Иногда преступники пытаются вызвать у потенциальных дропперов чувство жалости и объясняют, что сами не могут завести карту из-за проблем с долгами, поэтому им приходится обращаться за помощью к посторонним.

4. Убеждают внести переданные преступниками (а чаще — другими дропперами) наличные деньги на карту, а затем перевести их по указанным реквизитам. Стандартная ситуация, когда мошенник подходит к ребенку или подростку возле банкомата и объясняет, что ему нужно срочно отправить перевод другу / родственнику, но нужный банкомат или карта не работают. После чего он просит жертву внести наличные на свой счет и перевести другому человеку, как правило — за небольшое вознаграждение.

5. Требуют «вернуть» или перевести дальше средства, поступившие на личную карту. При этом на счет ничего не подозревающего подростка поступает денежный перевод. Затем на связь выходят злоумышленники и ссылаются на то, что перевели деньги по ошибке, и просят отправить их по «правильным» реквизитам либо «вернуть» владельцу (а на самом деле — также передать дальше по преступной цепочке).

6. Просят обналичить поступившие дропперу незаконно полученные деньги и затем передать их другому лицу. Схема действий киберпреступников та же, что и в предыдущем пункте, однако они просят не переводить средства, а снять их и передать «курьеру». Также они могут обратиться к ребенку возле банкомата, рассказывая о том, что не могут сами снять наличные по техническим причинам. После чего жертву просят «помочь» за вознаграждение и на месте обналичить переведенные на его счет средства.

Важно! С того момента, как дети попадаются на одну из этих уловок и помогают мошенникам в движении нелегально полученных средств, они становятся невольными соучастниками преступления.

Почему дети становятся «легкой добычей» злоумышленников?

Для мошенников не имеет значение, кто выступает в роли дропперов: их жертвами становятся и пенсионеры, и люди среднего и молодого возраста. Однако случаи, когда детей привлекают к незаконным финансовым операциям, в последнее время происходят все чаще.

Несовершеннолетние лица легче подвергаются манипуляциям по нескольким причинам:

1. Доверчивость. Большинство детей и подростков привыкли доверять взрослым и не ждут от них обмана. Предлагаемые преступниками действия напрямую не угрожают их личной безопасности, а желание подзаработать и помочь другим заставляет забыть об осторожности.

2. Недостаток жизненного опыта. Большинство детей растет в благополучной среде, имеет ограниченный круг общения (школа, секция, друзья) и попросту не сталкивается с преступлениями и нарушением чьих-то прав в повседневной жизни. Многие подростки даже не подозревают о том, что их могут обманом вовлечь в уголовно наказуемое деяние.

3. Незнание законодательства. Далеко не все дети могут похвастаться знанием российских юридических норм, и не видят ничего противозаконного в просьбе незнакомцев перевести или обналичить чужие средства.

4. Отсутствие финансовой грамотности. Зачастую родители заводят детям личные банковские карты еще задолго до наступления совершеннолетия, однако не уделяют должного внимания воспитанию финансовой грамотности и правил обращения платежными средствами, а также конфиденциальной финансовой информацией.

5. Боязнь показаться плохим человеком в глазах других. Вступая в контакт с потенциальной жертвой, злоумышленники умеют найти ее слабые психологические стороны, убедить и надавить на жалость. Отказ в помощи может заставить ребенка чувствовать себя виноватым и неполноценным в глазах окружающих.

Еще одна причина, по которой дети становятся дропперами — желание заработать. Многие подростки стремятся обрести финансовую независимость, или, как минимум, подзаработать денег на личные нужды. Киберпреступники активно пользуются таким желанием, и вовлекают несовершеннолетних лиц в дропперство под видом удаленной работы, курьерской деятельности и т. д.

Какое наказание грозит дропперам?

1. Ответственность за участие в дропперстве может грозить как самим несовершеннолетним лицам, так и их родителям. Согласно статье 1102 Гражданского кодекса РФ, гражданин, уличенный в незаконных финансовых операциях, обязан возместить потерпевшему ущерб за неосновательное обогащение. Если же дроппер еще не достиг совершеннолетнего возраста, ответственность за его поступок несут родители или иные законные представители (ст. 1072 ГК РФ).

2. С 16 лет юные дропперы могут уже самостоятельно нести уголовную ответственность за участие в незаконной деятельности: оно может быть квалифицировано как мошенничество (ст. 159 Уголовного кодекса РФ), легализация средств, полученных преступным путем (ст. 174 УК РФ), незаконная банковская деятельность (ст. 172 УК РФ).

За данные преступления предусмотрено наказание в виде лишения свободы и крупных штрафов.

5 июля 2025 года вступили в силу поправки, которыми вводится прямая уголовная ответственность за так называемое дропперство. Изменения внесены в статью 187 УК РФ «Неправомерный оборот средств платежей».

Теперь закон предусматривает ответственность для тех, кто за деньги передает свою банковскую карту для криминальной деятельности

или за вознаграждение сам совершает незаконные операции по указанию другого лица». **За это предусмотрено наказание от 3 до 6 лет лишения свободы со штрафами до 1 миллиона рублей.**

Признаки «ловушек» для вовлечения в дропы

1. Уверяют, что можно заработать большие деньги, прилагая минимум усилий.

2. Для получения «работы» нужно предоставить (передать или продать) свою банковскую карту или оформленную на вас сим-карту или сдать в аренду аккаунт в соцсетях/месенджерах.

3. Для заработка нужно принять на свою карту и обналичить денежный перевод или отправить полученный денежный перевод еще куда-либо.

4. Супервыгодное предложение о «работе» поступило через социальные сети, мессенджеры или электронную почту, а отправитель вам незнаком.

Как уберечь детей от вовлечения в дропперскую деятельность?

Чтобы ребенок не стал жертвой аферистов, рекомендуется соблюдать несколько простых рекомендаций:

1. Если подросток желает быть финансово самостоятельным, помогите ему с поиском подработки. Опытный взгляд взрослого человека поможет ему различить вакансии от реальных работодателей и «ловушки», размещенные мошенниками.

2. Необходимо уделять время изучению законов и ответственности за правонарушения. Познакомить ребенка с одним из главных принципов юриспруденции — что незнание закона не освобождает от ответственности. Кроме того, подросток должен осознавать, что несовершеннолетний возраст не дает ему привилегии безнаказанно совершать преступления: наказание, так или иначе, придется нести или ему самому, или родителям.

3. Следует прививать ребенку культуру обращения с деньгами и финансовую грамотность. Объяснять, что такое конфиденциальные платежные данные и почему их нельзя передавать третьим лицам. Приучайте подростка тратить деньги разумно, а крупные расходы согласовывать с вами.

4. Если у детей уже есть платежные карты, нужно контролировать совершаемые ими финансовые операции. Для этого следует подключить услугу двойного SMS-информирования о транзакциях: сегодня она доступна уже во многих банках. Благодаря такой функции можно получать оповещения обо всех поступлениях и расходах по карте ребенка. Если проведенные операции по ней покажутся подозрительными, можно сразу обратиться в банк или полицию.

Не обязательно оформлять банковский счет для подростка на его имя: достаточно выпустить для него карту-дублер, привязанную к счету родителя. Установите по ней небольшой лимит расходов (в том числе переводов, снятия наличных): это обезопасит от необдуманных действий ребенка, если он все же поддастся уловкам мошенников.

Как узнать, что ребенка втянули в махинации?

Согласно изменениям, внесенным 24.06.2025 в Гражданский Кодекс Россйсикой Федерации, несовершеннолетние в возрасте от четырнадцати до восемнадцати лет вправе открыть банковский счет только с согласия родителей или законных представителей.

Банк России установил требования, по которым банки должны уведомлять родителей, если их детям в возрасте от 14 до 18 лет выдается банковская карта. Более того, родители смогут отслеживать все операции и расходы, совершаемые подростком по этому счету. Способ информирования прописывается в договоре с банком. Также родители могут оформить совместные СМС-уведомления, чтобы контролировать финансовые операции ребенка, — некоторые крупные банки предоставляют такую возможность.

Также родители или законные представители могут обратиться в налоговую инспекцию, им предоставят информацию обо всех открытых счетах и операциях несовершеннолетнего. Или они могут подключить своего ребенка к своему Личному кабинету налогоплательщика.

Памятка

Даже самое маленькое необдуманное действие может поломать не только карьеру, но и судьбу, а также создать массу проблем близким, связанных с взысканием имущества, осуждением окружающими, невозможностью трудоустройства на хорошую высокооплачиваемую работу.

Не бери чужие вещи – это нечестно!

Не доверяй незнакомцам!

Никогда не открывай незнакомые ссылки!

Не говори незнакомцам свой адрес и телефон!

Если что-то кажется подозрительным – расскажи взрослым!

Всегда спрашивай разрешения у родителей!

Помни: настоящие друзья не просят ничего плохого!

Если что-то не так – сразу расскажи маме или папе!

Будь осторожен в интернете – там могут быть плохие люди!

Примеры

1. Организатор из Москвы

Что произошло: *в Москве впервые завели уголовное дело на организатора дропперской схемы. Его поймали после того, как один из его «дропов» пошел на сделку со следствием и сдал его.*

Как работала схема: *мужчина скупал банковские карты и счета у других людей, а затем продавал их или использовал для преступных операций. По сути, он создал черный рынок банковских карт.*

Чем всё кончилось: у него дома нашли мешки банковских карт, сим-карт и техники. Теперь ему грозит серьезный срок по статье 187 УК РФ (незаконный оборот средств платежей). Дело расследуется.

2. Подросток из Нижегородской области

Что произошло: *20-летний парень из города Семёнова втянул в преступный бизнес своего 15-летнего друга.*

Как работала схема: *старший нашел в мессенджере предложение о «легких деньгах» и предложил знакомому подростку заработать. Всё, что нужно было сделать — сходить в банк, оформить на себя карту и отдать ее вместе с паролями. За это подросток получил несколько тысяч рублей.*

Чем всё кончилось: *организатор (20 лет) пойдет под суд по уголовной статье. На родителей подростка составили протокол за то, что они плохо следят за ребенком (статья 5.35 КоАП РФ — неисполнение родительских обязанностей). Теперь им грозит штраф.*

3. Офис дропов в Челябинске

Что произошло: *полиция накрыла в Челябинске настоящий офис, который работал как конвейер по сбору банковских карт. Там была выстроена целая иерархия: руководитель, бригадир, старший менеджер и простые дропы.*

Руководительница (1999 г.р.) — управляла всем процессом, общалась с заказчиками в интернете.

Бригадир (2006 г.р.) — командовал теми, кто приносил карты.

Старший менеджер (2008 г.р.) — проверял, работают ли карты, и проводил операции.

Дропы — два парня 2007 и 2008 г.р., которые просто продали свои карты и получили за это до 5000 рублей каждый.

Чем всё кончилось: *всем организаторам грозят уголовные сроки (кто-то уже под домашним арестом). А продавцы карт (дропы) теперь тоже под следствием. Им грозит до 6 лет лишения свободы по ч. 3 ст. 187 УК РФ. За пять тысяч рублей.*

4. Школьник перевел почти миллион с карты родственника

Что произошло: *мошенники убедили 12-летнего ребенка перевести огромную сумму денег. Это дело вскрыло целую сеть преступников по всей России.*

Как работала схема: *ребенку (2012 г.р.) позвонили мошенники и уговорили оформить карту на имя родственника и перевести на «безопасный счет» 865 000 рублей. Деньги упали на карту 18-летнего парня (2006 г.р.), который был дроппером. Он поехал в другой регион и снял все наличные в банкомате.*

Чем всё кончилось: *полиция вышла на след и задержала троих организаторов (2004–2006 г.р.). У них нашли десятки карт и сим-карт, телефоны с перепиской, где они обсуждали «залив» денег и их обналичивание.*

Оказалось, что эта группа причастна как минимум к восьми мошенничествам в разных регионах (Москва, Пермь, Белгород и др.). Ущерб по каждому эпизоду — от 150 тысяч до 2 миллионов рублей. Организаторов отправили в СИЗО.

Аренда аккаунтов

Использование аккаунтов в мессенджерах — это распространенная схема, которую мошенники применяют для маскировки своей деятельности.

Основная категория лиц, вовлекаемых в указанную противоправную деятельность – учащиеся образовательных организаций, которые за денежное вознаграждение временно предоставляют доступ к своим аккаунтам.

Злоумышленники обещают легкий доход за простое действие — передачу логина и пароля или кода аутентификации, тем самым вовлекая детей в соучастие в преступлении.

Преступники ищут легкие способы получения доступа к верифицированным профилям, чтобы использовать их как инструмент для организации и совершения различных видов преступлений, в том числе тяжких и особо тяжких (рассылка вредоносных ссылок, организация фишинговых атак, вывод незаконно полученных денежных средств, мошенничество, организация террористических и диверсионных актов, вербовка в противоправную деятельность), от которых также могут пострадать родственники ребенка, сдавшего свой аккаунт в аренду.

Поиск желающих сдать свой аккаунт в аренду осуществляется злоумышленниками через различные мессенджеры, социальные сети и чаты онлайн-игр.

Дополнительную опасность представляет эффект вторичного вовлечения: получив первое вознаграждение, подростки начинают рекомендовать данный способ «заработка» сверстникам и одноклассникам, что способствует быстрому распространению противоправной практики внутри школьной среды.

В 2025 году выявлено более 700 тыс. уникальных абонентских номеров, на которые зарегистрированы аккаунты в различных мессенджерах, сданные в аренду для совершения с их использованием преступлений.

Уголовная и административная ответственность

Передача доступа к своему аккаунту третьим лицам не освобождает владельца от ответственности. Даже если ребенок не осознавал корыстных целей заказчика, его профиль становится цифровым следом, ведущим к нему как к соучастнику. В зависимости от тяжести содеянного, последствия могут варьироваться от блокировки всех связанных сервисов до постановки на учет в правоохранительных органах и привлечения ребенка либо его родителей к административной или уголовной ответственности.

С 1 сентября 2025 года вступили в силу изменения, внесенные в Уголовный Кодексе Российской Федерации и Кодекс Российской Федерации об административных правонарушениях.

Введена ст. 274.5 УК РФ, устанавливающая ответственность за организацию или участие в деятельности по передаче информации, необходимой для регистрации или авторизации пользователя сети «Интернет» для получения доступа к функциональным возможностям

информационного ресурса, если эти деяния совершены из корыстной заинтересованности либо в целях совершения иного преступления.

Введена ст. 13.29.2 КоАП РФ, устанавливающая ответственность за передачу информации, необходимой для регистрации и (или) авторизации пользователя информационно-телекоммуникационной сети «Интернет» для получения доступа к функциональным возможностям информационного ресурса, иному лицу, если эти действия не содержат признаков уголовно наказуемого деяния.

В случае недостижения участником преступной схемы по аренде аккаунтов возраста уголовной ответственности, к ответственности будут привлечены его родители **по статье 5.35 КоАП РФ.**

Справочно: в настоящее время возбуждены пять уголовных дел в отношении пяти лиц, в отношении 10 (моложе 16 лет) проведены профилактические мероприятия (5 поставлены на учет в ПДН).

Последствия сдачи своего аккаунта в аренду

Личный аккаунт в мессенджере — это такая же персональная ценность, как ключ от квартиры. Передача управления своим профилем чужому человеку фактически означает соучастие в совершении преступления.

Когда преступники используют чужой аккаунт, они фактически используют цифровую личность человека. Для правоохранительных органов цепочка доказательств в первую очередь указывает на того, на чье имя или номер телефона зарегистрирована учетная запись.

Это создает серьезные риски: от репутационных потерь до реального уголовного преследования, поскольку доказать свою непричастность к действиям, совершенным из-под собственного подтвержденного профиля, крайне сложно.

В Интернете нет анонимности. Любое преступление, совершенное в интернете, оставляет цифровой след, который в ходе расследования всегда приведет к тому, кто его оставил. Любые действия, совершенные через верифицированный профиль, технически и юридически привязываются к его владельцу.

Аренда аккаунтов — это не «подработка», а реальное участие в преступлении. Когда человек передаёт свой аккаунт, номер телефона и коды авторизации, он передаёт инструмент совершения преступления.

Даже если подросток не разговаривает с потерпевшими, не держит в руках похищенные деньги и «ничего плохого сам не делает», он становится частью преступной цепочки.

Передача личной информации незнакомым людям недопустима, так как это может привести к вовлечению в незаконную деятельность.

Справочно: самый молодой установленный участник преступной схемы – десятилетний Н., предоставивший свой аккаунт кол-центру за 1,5 тыс. рублей. Анонимные работодатели предупредили его о своих намерениях и убедили в том, что сделка безопасна. Однако в результате школьник

фактически стал соучастником преступлений, совершенных в составе организованной группы, что является отягчающим обстоятельством.

Как распознать мошенников

«Это совершенно законная возможность заработать! Но знай, лучше никому не говори, чтобы твои конкуренты не узнали твой секрет успеха», — такими словами мошенники пытаются привлечь жертв.

СТОП фразы

Если в общении с незнакомцем вы слышите следующие фразы, это явный признак мошенничества. Необходимо срочно прекратить диалог и сообщить родителям:

«Никому не говори», «Легко заработать», «Это полностью законно», «Аренда/доступ к аккаунту».

Рекомендации

Никогда не передавать логины, пароли и коды из СМС для двухфакторной аутентификации третьим лицам, под каким бы предлогом их ни просили.

Регулярно проверять раздел «Активные сессии» или «Устройства» в настройках мессенджеров, чтобы убедиться, что к аккаунту не подключены посторонние лица.

С осторожностью относиться к предложениям о покупке или аренде аккаунтов. Подобные сделки в 100% случаев связаны с противоправной деятельностью.

Критически оценивать предложения о «легком заработке» в интернете, которые требуют выполнения простых технических действий с личными данными или социальными сетями.

Примеры

1. Юный администратор из Астрахани

Что произошло: в Астрахани нашли 15-летнего подростка (2009 года рождения), который управлял целым Telegram-каналом по сдаче чужих аккаунтов в аренду. По сути, он был связующим звеном между владельцами симок и мошенниками.

Как работала схема: парень собирал у желающих «подзаработать» номера телефонов и коды подтверждения из СМС. Всё это он тут же переправлял в мошеннический кол-центр. Там с помощью этих данных регистрировали новые аккаунты в мессенджерах или получали доступ к существующим. За свою «работу» участники получали деньги в криптовалюте. Всего через канал подростка прошло более 100 номеров.

Какие последствия: полиция выяснила, что минимум один из этих номеров использовался для реального мошенничества — по этому факту уже возбуждено уголовное дело на самих мошенников. А организатору схемы (тому самому подростку) теперь предъявлено обвинение по статье 274.5

УК РФ. Доказательства железные: переписки, номера, коды и переводы крипты сохранились.

2. Обезличенный допрос фигуранта

Что произошло: В июне 2025 года осужденный сидел у мамы дома и играл в PUBG. В чате игры написал какой-то игрок и предложил заработок, обсуждение перешло в Telegram.

Как работала схема: оказалось, что нужно находить сим-карты (любого оператора) и сдавать их в аренду. Номер мог быть нужен на время.

Чем дольше аренда — тем дороже. Цены были от 3 до 10 долларов. Чтобы «сдать» номер, нужно было ловить СМС с кодом подтверждения для регистрации в мессенджере (WhatsApp, Telegram и др.) и сразу отправлять код заказчику. Код действует всего минуту. Оплата шла в крипте (USDT) посредством специального бота.

В первый раз был отправлен код из СМС для входа в WhatsApp. По инструкции он целый день не заходил в свой аккаунт, чтобы якобы не сбить настройки. За это перевели 3-4 доллара. Крипту через обменник он перевел на свою карту. На следующий день зашел в свой Telegram, тем самым отвязав чужое устройство, и продолжил пользоваться сам, думая, что всё чисто.

На следующий день тот же куратор написал снова. Сказал, что есть схема выгоднее: я могу быть не просто «сдатчиком», а «дроповодом». Задача — искать других людей («дропов»), которые будут сдавать свои номера. С каждого такого «дропа» капало 50 центов комиссии.

После предложили создать собственный Telegram-канал, чтобы зарабатывать больше. Схема простая: мы покупаем доступ к аккаунтам у дропов за 2 доллара, а перепродаем за 4. Он согласился и стал администратором канала, где сидело около 100 человек. Все они скидывали номера и коды. Канал работает до сих пор. Все собранные номера скидывал «скупщику» в другом, закрытом чате.

ДЕСТРУКТИВНЫЙ КОНТЕНТ

Статистические сведения

В 2025 году Роскомнадзором заблокирован доступ к 1,289 млн запрещённых и деструктивных материалов, что на 59 % больше, чем годом ранее (в 2024 году заблокировано 810 тыс. таких материалов).

Зафиксирован существенный рост блокировок материалов, содержащих контент, связанный с ЛГБТ-тематикой — в 3,7 раза (до 170,3 тыс.) и детской порнографией - в 2,3 раза (до 155,6 тыс.).

МВД России совместно с Роскомнадзором ограничен доступ к более чем 150 тыс. сайтов и страниц, содержащих пронаркотический контент, а также информацию о способах изготовления взрывчатых веществ, взрывных устройств и оружия.

Преступления

В 2025 году на территории России преступным посягательствам с использованием информационно-коммуникационных технологий подверглось 534 444 лиц, из которых – 13 017 несовершеннолетних. В 4,3 раза возросло количество фактов, где потерпевшими по ***главе 28 УК РФ*** *стали несовершеннолетние - 1 071.*

Количество ***суицидов****, совершенных в 2025 году – 795 (2024 г. - 735), попыток – 104 (2024 г. — 90). Количеств фактов* ***изготовления порнографических материалов*** *с несовершеннолетними — 434 (2024 г. — 905). Количество фактов против* ***половой неприкосновенности*** *несовершеннолетних — 1629 (2024 г. — 1 996). Склонение к потреблению* ***наркотических средств****, псих. веществ или аналогов – 15 (2024 г. — 5).*

Отмечается тенденция к росту подростковой преступности, связанной с незаконным оборотом ***наркотиков – 992*** *(2024 г. - 900) лица, по преступлениям, предусмотренным* ***статьей 207 УК РФ*** *(заведомо ложное сообщение об акте терроризма) –* ***192*** *(2024 г. - 142) лица, а также по преступлениям, связанным с неправомерным* ***оборотом средств платежей – 34*** *(2024 г. - 19).*

Установленное ***количество фактов по ст. 207 УК РФ****, совершенных несовершеннолетними или при их соучастии (предварительно расследованные преступления) –* ***287****.*

Деструктивный контент (от лат. destructio — разрушаю) — это информация в интернете, которая наносит вред психическому или физическому здоровью человека, а также негативно влияет на его поведение и восприятие реальности. В отличие от обычного контента, который может быть скучным или бесполезным, этот вид материалов намеренно или косвенно подталкивает зрителя к опасным действиям или искажает его моральные ориентиры.

Виды деструктивного контента:

Контент наносящий непосредственный вред жизни и здоровью ребенка *(суицидальный контент, селфхарм, группы анорексии и т.д.);* Контент наносящий вред психическому здоровью ребенка, провоцирующий нервные расстройства *(шок-контент, депрессивный контент, эзотерика, окультизм, группы, пропагандирующие эксперименты над психикой);*

Контент, склоняющий ребенка к преступным действиям и насилию *(колумбайн, АУЕ, сатанисты);*

Контент наносящий урон морально-этическому состоянию ребенка, разрушающий семейные ценности, настраивающий ребенка против родителей (*феминистки, чайлдфри, аморальный юмор);*

Развращающий контент, склоняющий ребенка к смене ориентации или пола, пропагандирующий иные виды извращений (*ЛГБТ, смена пола);*

Манипулятивный контент — цель получение материальной выгоды с ребенка *(Ставки на спорт, букмекерские конторы, онлайн-казино, вейпы, снюсы, электронные сигареты, онлайн игры).*

К наиболее опасному контенту относится:

Депрессивный контент. Такой контент в социальных сетях является базой, отправной точкой для формирования различных типов асоциального поведения. Сообщества, размещающие у себя депрессивный контент популяризируют и романтизируют психическое расстройство. Пользователи таких сообществ часто сами себе приписывают депрессивное состояние, гордятся им.

Суицидальный контент. Визуальная информация, популяризирующая и призывающая к совершению самоубийства, рассказывающая о способах совершения суицида. Существуют сообщества нескольких типов. Первый тип – юмор на тему суицида или около-юмористический контент. Второй тип – сообщества с депрессивным контентом без явных призывов к совершению самоубийства. Третий тип – закрытые сообщества с контентом, направленным уже на само совершение суицида.

Контент, популяризирующий употребление ПАВ (наркотики, табак и алкоголь, снюс и вейп).

Экстремизм, нацизм и терроризм (визуальный контент, направленный на устрашение другой нации или расы, вытеснение ее представителей в низшие касты, уничтожение ее культуры).

ЛГБТ–сообщества (содержание данного контента очень сильно влияет на половую идентификацию подрастающего поколения. Призывает к смене пола и другим проявлениям, свойственным лицам с нетрадиционной ориентацией).

«Группы смерти» (участники данных групп подталкивали друг друга к самоубийству, либо же следовали указаниям куратора-итог заданий-смерть).

Колумбайн (субкультура «Колумбайн» — это способ подросткового суицида, в котором подросток пытается покончить с собой, отомстив своим обидчикам).

Скулшутинг – следствие увлечения субкультурой Колумбайна, вооруженное в нападении учащегося или стороннего человека на школьников внутри учебного заведения.

Кибербуллинг (интернет травля).

Последствия влияния деструктивного контента на реальную жизнь подростка:

1. Снижение успеваемости или отказ от посещения занятий; систематические прогулы занятий.
2. Ухудшение самочувствия и здоровья в целом.
3. Непризнание авторитетов в лице взрослых.
4. Агрессивное, обесценивающее, игнорирующее, снисходительное отношение учеников к учителю, запугивание и травля учениками учителя.
5. Формирование школьных банд.
6. Попадание в руки педофилов.
7. Потеря персональных данных.

Кто особенно подвержен риску интернет-атак:

дети, родители которых чрезмерно заняты и не контролируют время, проведенное детьми в интернете.

подростки, в силу своих возрастных особенностей («тяга испробовать все и вся»);

подростки, страдающие тяжелыми соматическими или психическими заболеваниями (кибербуллинг);

подростки с повышенной тревожностью, зацикленные на негативных эмоциях, склонные к депрессиям (суицидальный и депрессивный контент).

Механизм влияния таких материалов часто строится на эмоциях.

Авторы используют шокирующие заголовки и яркие образы, чтобы заставить пользователя досмотреть видео до конца или вступить в спор в комментариях. Для алгоритмов социальных сетей бурная реакция зрителя является сигналом популярности, поэтому вредные ролики могут быстро распространяться и попадать в рекомендации.

Длительное потребление разрушительной информации может привести к потере уверенности в себе, появлению агрессии к окружающим или глубокому стрессу. Распознавание таких материалов помогает сохранять критическое мышление и поддерживать экологичную информационную среду вокруг себя.

Этапы установления психологического контроля над человеком:

Этап дестабилизации: выведение человека из состояния равновесия, повышение внушаемости посредством воздействия на защитные механизмы, внушение сомнения в привычных представлениях о реальности и себе.

Этап замены: после того как человек начинает сомневаться в своих прежних убеждениях, вводятся новые идеи, ценности или поведение, которые усиливают контроль над сознанием личности. Это осуществляется через внушение, повторение и создание зависимости от деятельности группы.

Этап подкрепления: закрепление новой системы ценностей и убеждений, включение личности в деятельность деструктивной группы, что формирует новые смысловые ориентиры. Использование контроля для поддержания зависимости личности от группы.

Как распознать деструктивный контент?

Распознавание деструктивного контента требует внимательности к деталям и критического анализа поступающей информации.

Первым признаком является резкая эмоциональная реакция, которую пытается вызвать автор: если после прочтения или просмотра возникают сильное чувство тревоги, страха, гнев или ненависть к определенной группе людей, вероятно, контент создан для манипуляции.

Важно обращать внимание на способ подачи материала. Деструктивные сообщения часто содержат ультимативные утверждения, не допускающие сомнений, или делят мир на «черное и белое», «своих и чужих».

Использование шокирующих заголовков, которые не соответствуют содержанию, а также обильное использование агрессивной лексики и капслока служат индикаторами токсичной информационной среды.

Следует анализировать предлагаемые действия. Если контент призывает к изоляции от близких, отказу от критического мышления, участию в опасных для здоровья активностях или оправдывает насилие как единственный способ решения проблем, это явные признаки опасности.

Отсутствие ссылок на проверяемые источники или ссылки на анонимные ресурсы также должны вызывать подозрение.

Деструктивный контент может романтизировать депрессивные состояния или рискованные поступки, представляя их как признак исключительности или силы духа. Деструктивная группа, как правило, является закрытой, чтобы придать оттенок «исключительности» и «эксклюзивности информации».

Понимание этих признаков позволяет вовремя прекратить взаимодействие с вредным ресурсом.

Как ребенку самостоятельно защититься от деструктивных сообществ?

Будьте критичны. Если вам что-то предлагают, навязывают, требуют, необходимо задать вопрос самому себе: какую цель преследует собеседник.

Оставайтесь на связи. Поддерживайте контакты с семьей, друзьями и обществом в целом. Это поможет вам сохранить критичность мышления и не поддаться влиянию группы.

Осознанно принимайте решения. Анализируйте, на какой информации
вы основываетесь при принятии решений, сколько источников используете, принимаете ли во внимание последствия.

Не бойтесь задавать вопросы. Если вам предлагают присоединиться к группе, не стесняйтесь спрашивать о правилах, целях и последствиях выхода из сообщества.

Сверяйтесь со своими эмоциями. Если что-то кажется вам подозрительным или неправильным, доверяйте своему чувству. Обратите внимание, если Ваше эмоциональное состояние.

Важно быть осведомленным о признаках деструктивных сообществ и оказывать поддержку тем, кто может оказаться в опасной ситуации. Если вы или кто-то, кого вы знаете, сталкивается с подобной проблемой, рекомендуется обратиться за помощью к близким, друзьям, специалистам или организациям, занимающимся вопросами обеспечения безопасности личности, в том числе и психологической.

Правило четырех пальцев (чек-лист):

Стоп: выключи экран или перелистни. Не досматривай до конца.

Блок: заблокируй источник и отправь жалобу модераторам (кнопка «Пожаловаться»).

Тишина: не комментируй и не пересылай это друзьям. Твой гневный комментарий только поможет видео стать популярнее.

Голос: если тебе страшно или тревожно — расскажи об этом родителям или учителю.

Памятка для ребенка

Никогда не вступай в переписку с агрессорами. Им нужна твоя реакция.

Твои данные — это ключи от дома. Не давай незнакомцам свой номер телефона и адрес.

Скриншот — твой свидетель. Если тебя обижают, сохрани доказательство.

Кнопка «Пожаловаться» — это не ябедничество, а помощь соцсети стать чище и безопаснее.

Информация, побуждающая к нанесению вреда себе или другим, содержащая призывы к жестокости или употреблению запрещенных веществ, запрещена Федеральным законом №436 «О защите детей от информации, причиняющей вред их здоровью и развитию», а также формирует негативный цифровой след.

Примеры

1. Смертельные игры в Telegram: как подростков толкают к суициду?

Что произошло: *полиция нашла в мессенджере закрытую группу, которая толкала подростков к самоубийству. Организатором оказался молодой человек 2004 года рождения (сейчас ему около 20 лет). Он создал сообщество, где постепенно, шаг за шагом, доводил детей до отчаяния.*

Мотивы: *не какая-то высокая идея, а обычное больное самолюбие. Ему нравилось чувствовать власть над людьми, наблюдать, как они ломаются и подчиняются. Он втирался в доверие к подросткам, жалел их, обсуждал с ними, как всё плохо, какой мир несправедливый и какая жизнь бессмысленная. Дети попадали в эмоциональную зависимость от этого общения.*

Как работала схема: *в группе давали «задания». Например, одна девятиклассница под влиянием администратора начала резать себе руки и снимать это на видео — как доказательство, что она «своя» и готова на всё. Чем дальше, тем страшнее становились задания.*

Со временем девочка сама стала частью системы — её сделали модератором. Она уже помогала вести переписку, «поддерживала» новых участников (то есть затягивала их туда же) и повторяла те жуткие вещи,

которые говорил организатор. Другие дети приходили в группу из любопытства или за острыми ощущениями, а попадалив психологическую ловушку.

Какие последствия: *полиция успела сработать вовремя. Выяснилось, что как минимум две девушки — школьница и студентка колледжа — уже дошли до финальной стадии суицидальной игры и нанесли себе серьезные травмы. Им оказали психологическую помощь, буквально вытащили с того света. Организатора задержали. На него завели уголовное дело по статье 110.2 УК РФ (склонение к самоубийству). Ту самую девятиклассницу тоже привлекли к ответственности — теперь она не жертва, а соучастница.*

2. Друг из чата оказался вербовщиком: история про поджог и СИЗО.

Что произошло: *в Санкт-Петербурге подростка поймали на попытке поджечь железнодорожный локомотив. Парень не экстремист и не террорист — он просто попался на удочку взрослого человека, который притворился его другом.*

Мотивы: *подросток сидел в тематическом интернет-чате. Там с ним познакомился пользователь, представился ровесником. Они начали общаться, обсуждать жизнь, политику, «несправедливость государства». Собеседник был умным, понимающим, подбирал нужные слова. Постепенно от простых разговоров и мемов перешли к делу: «А давай не просто болтать, а покажем всем нашу позицию?»*

Как работала схема: *«друг» оказался дистанционным куратором. Он никогда не появлялся лично, но шаг за шагом вел подростка:*

- Объяснил, что именно поджечь (локомотив — хорошая цель).

- Рассказал, в какое время это делать, чтобы не поймали.

-Дал инструкции по конспирации: как подойти, что надеть, как уйти.

Сам он при этом сидел далеко и в безопасности. Когда подростка задержали на месте с поличным, полиция провела экспертизу переписки. И выяснилось: «друг» никакой не ровесник. Это взрослый мужчина, который специально использовал психологические приемы и речевые конструкции, чтобы втереться в доверие. Кто он такой — найти не смогли, следы затерялись в сети.

Какие последствия: *подростка арестовали. Он сейчас в СИЗО. Ему грозит статья за покушение на террористический акт (ч. 3 ст. 30 – п.п. «а, в» ч. 2 ст. 205 УК РФ). Он признал вину, но это не отменяет того факта, что его жизнь сломана. А настоящий преступник, который им управлял, остался на свободе и уже ищет следующую жертву.*

3. Хайп ценой жизни: трюк на крыше автомобиля

Что произошло: *17-летний парень решил стать звездой соцсетей. Он залез на крышу движущейся машины, попытался перебраться на пассажирское сиденье, отпустил руль, сорвался и упал прямо на дорогу. Чудом остался жив и не попал под колеса.*

Мотивы*: подростки сидели в интернет-сообществе, где обсуждали экстремальные трюки и челленджи. Там царила атмосфера «сними что-то*

жёсткое, получи хайп, собери подписчиков». Любой ценой, чем опаснее — тем круче. Парень повелся на это. Ему хотелось выделиться, доказать, что он смелый, получить признание.

Как работала схема: н*икаких мошенников и кураторов — просто токсичная среда и глупость. Парень взял без спроса машину родственника, выехал на дорогу и решил повторить трюк, который видел в интернете. Он думал, что это будет эффектное видео для его страницы. Вместо этого он чуть не погиб.*

Какие последствия: *сам подросток: чудом остался жив, но теперь ему светят административные протоколы за грубейшее нарушение ПДД. И главное — он не сможет получить водительские права ближайшие несколько лет.*

Машина: угнанный автомобиль родственника отправили на штрафстоянку.

Родители: решается вопрос о привлечении их к ответственности.

Друг: знакомый, который был в курсе и подтвердил реальность видео (парень сначала пытался врать, что это нейросеть), тоже попал в поле зрения полиции.

Даже «развлекательный» деструктивный контент, создаваемый ради лайков и просмотров, способен привести к реальной угрозе жизни, правовым последствиям и вовлечению подростков в опасные практики, формирующие искаженную систему ценностей.

МЕДИАГРАМОТНОСТЬ И КИБЕРГИГИЕНА

Статистические сведения

В 2025 году количество зарегистрированных преступлений в сфере противоправного использования информационно-коммуникационных технологий составило 627 тысяч, из которых 65% пришлось на преступления мошеннического характера (против собственности) (430,9 тыс.).

Значительная часть преступлений в рассматриваемой сфере совершена с использованием сети Интернет – 564,7 тыс., средств мгновенного обмена сообщениями (интернет-мессенджеры) – 258,4 тыс. и методов социальной инженерии – 200,5 тыс. Общее количество потерпевших от преступлений в сфере информационно-коммуникационных технологий составило 534 444.

Почти двухкратное увеличение числа потерпевших среди несовершеннолетних связано с двумя факторами. Во-первых, в условиях цифровизации дети все в более раннем возрасте начинают пользоваться мобильными устройствами с возможностью выхода в сеть Интернет, где оставляют значительное количество своих персональных данных и цифровых следов. Во-вторых, злоумышленники постоянно совершенствуют методы социальной инженерии, позволяющие все изощреннее обманывать

граждан, в том числе несовершеннолетних, чей уровень критического мышления не позволяет в должной мере распознать обман.

В отношении несовершеннолетних злоумышленники чаще всего реализуют следующие схемы:

«Звонки от представителей образовательных организаций».

Под предлогом проблем с экзаменами (ЕГЭ), регистрацией на образовательных платформах злоумышленники выманивают коды авторизации или иную значимую информацию, далее звонят несовершеннолетнему, представляясь сотрудниками «Госуслуг», Банка России или правоохранительных органов, запугивают уголовной ответственностью и вынуждают сообщить данные платежных средств родителей либо передать наличные средства, ценности (золото, валюту) курьеру.

«Кража учетных записей».

Злоумышленники получают доступ к аккаунтам различных сервисов путем фишинговой рассылки, перехвата кодов доступа через включенную демонстрацию экрана или распространения вредоносного программного обеспечения. В дальнейшем злоумышленники используют доступ к аккаунту для совершения финансовых операций и получения персональной информации или, что более характерно для несовершеннолетних, похищают виртуальные ценности (игровые предметы).

«Мошенничество при онлайн-покупках».

Злоумышленники создают в мессенджерах поддельные магазины, предлагающие популярные у целевой аудитории товары (например, одежду, обувь) по заниженным ценам. После предоплаты за товар у жертвы требуют дополнительные средства под предлогом «таможенных пошлин» или иных сборов. После получения платежей связь прекращается, товар не поставляется.

«Онлайн-игры и виртуальные ценности».

Игровые онлайн-платформы регулярно используются злоумышленниками для поиска жертв и организации первоначального контакта с ними. В 2025 году непосредственно в игровых онлайн-сообществах зафиксировано порядка 1000 имущественных преступлений. Больше всего преступлений совершено с использованием платформы «Roblox», что связано с развитой внутренней инфраструктурой и наличием внутриигровой валюты (robux). В качестве предлога используются «подарки», «розыгрыши», «ограниченные предложения», «донаты» и «выгодные сделки».

«Блокировка учетной записи iCloud».

Мошенник подыскивает жертву, пользующуюся устройством «Apple», и выстраивает доверительные отношения. После чего направляет жертве фото разбитого телефона, объясняет, что не может войти в учетную запись «iCloud». Сообщает о необходимости распечатать билеты на самолет или материалы для доклада руководителю. Ввиду срочности

мошенник просит войти в его учетную запись, после чего блокирует устройство жертвы. Чаще всего блокировка осуществляется в целях вымогательства денежных средств. Угрозами выступают удаление данных или безвозвратная блокировка устройства, средняя сумма составляет около 10 тыс. рублей.

«Мошенничество в сфере трудоустройства».

Злоумышленники предлагают за вознаграждение выполнять не требующие квалификации задачи, например, добавлять товар в избранное на сайтах маркетплейсов, ставить «лайки» и оставлять комментарии.

Такие предложения распространяются в социальных сетях, мессенджерах или на платформах для бесплатных объявлений. На первом этапе для формирования доверия злоумышленники используют чаты, где обсуждаются рабочие задачи и доходы участников, а также выплачивают незначительные вознаграждения.

На втором этапе потерпевшим предлагают более сложные и высокооплачиваемые задачи. Под предлогом «выкупа товара», «повышения рейтинга интернет-магазина» или «активации задания» граждан побуждают перевести денежные средства, после чего контакты с мошенниками прекращаются.

«Мошенничество в сфере онлайн-знакомств».

Злоумышленники создают привлекательные профили в социальных сетях и на специализированных платформах, выстраивают доверительные отношения в течение нескольких дней или недель, демонстрируя заинтересованность, внимание и эмоциональную вовлечённость.

Далее под предлогом организации «первого свидания» мошенники предлагают приобрести билеты в театр, кино или на концерт, направляя потерпевшему ссылку на поддельный сайт оплаты.

Склоняют к обмену личными фотографиями или видеозаписями, после чего угрожают их распространением среди родственников, друзей или по месту учёбы и требуют денежные средства.

Получив геолокацию или персональные данные, мошенники связываются с потерпевшим от имени «правоохранительных органов» или «спецслужб», заявляя о якобы совершённых противоправных действиях (например, пособничестве террористической деятельности) и убеждают срочно передать денежные средства «для декларации», в том числе через курьеров.

Критическое мышление

Критическое мышление — это способность человека объективно анализировать информацию, ставить под сомнение утверждения и делать обоснованные выводы на основе фактов и логики. Оно помогает отделять правду от манипуляций, распознавать ошибки в рассуждениях и принимать взвешенные решения.

В эпоху огромного потока данных этот навык становится ключевым для понимания того, насколько достоверно то или иное сообщение. В интернет-

пространстве критическое мышление служит основным инструментом защиты от дезинформации и фейков.

Чтобы эффективно применять его в сети, важно не принимать на веру первое увиденное утверждение, а всегда проверять информацию в нескольких независимых источниках. Разные точки зрения и сопоставление данных из авторитетных СМИ, официальных отчетов и экспертных материалов позволяют сформировать более точную картину происходящего.

Оценка достоверности сайтов также играет важную роль: стоит обращать внимание на репутацию ресурса, наличие ссылок на первоисточники и дату публикации.

Если новость или предложение в интернете выглядят слишком подозрительно, вызывают чрезмерно сильные эмоции или кажутся нереалистичными, это повод проявить осторожность и провести тщательную проверку, прежде чем распространять такой контент или следовать его рекомендациям.

Базовые правила цифровой гигиены

Использовать сложные пароли. Не «123456» и не дату рождения. Пароль должен содержать прописные и строчные буквы, цифры и символы. Лучше — уникальный для каждого сервиса.

Включить двухфакторную аутентификацию. Даже если пароль утечёт, без дополнительного кода злоумышленник не получит доступ к аккаунту.

Устанавливать приложения только из официальных магазинов. Сторонние сайты часто распространяют программы-шпионы, которые перехватывают данные.

Пользоваться отдельной картой для онлайн-платежей. Виртуальная или дополнительная карта с ограниченным балансом снижает риски при компрометации данных.

Настроить приватность в соцсетях и мессенджерах. Ограничьте круг лиц, которые видят ваши публикации, номер телефона и личную информацию.

устройствах.

Если доступ к компьютеру получит посторонний, он автоматически войдёт в ваши аккаунты.

Не использовать публичный Wi-Fi для банковских операций. В открытых сетях данные могут быть перехвачены.

Не переходить по неизвестным ссылкам. Фишинговые сайты выглядят как настоящие банки или «Госуслуги», но созданы для кражи данных.

Не отправлять фото документов и коды из СМС. Код подтверждения — это ключ к вашему аккаунту. Его никогда не запрашивают сотрудники банков или ведомств.

Не публиковать избыточную личную информацию. Адрес, геолокация, данные о семье и поездках — это материал для социальной инженерии.

Советы по защите от приемов социальной инженерии

Проверять любую информацию через официальный источник. Если звонят «из банка» — положите трубку и перезвоните по номеру с официального сайта. Если пишут «из вуза» — уточните у преподавателя или в деканате.

Брать паузу. Фразы «срочно», «прямо сейчас», «иначе будет поздно» — главный маркер манипуляции. Законные организации не требуют немедленных действий под угрозой.

Обсуждать подозрительные ситуации с близкими. Мошенники всегда требуют сохранить «секрет». Любое требование никому не рассказывать — тревожный сигнал.

Разделять онлайн и реальную жизнь. Человек в мессенджере — не обязательно тот, за кого себя выдает. Фото, голос, видеосвязь могут быть поддельными.

Использовать принцип нулевого доверия. Это означает: *по умолчанию не доверять никому в сети, пока информация не подтверждена*. Даже если собеседник представляется одноклассником, сотрудником полиции или «новым другом».

Не сообщать коды из СМС, пароли и данные карт — никому. Ни «банку», ни «службе безопасности», ни «следователю».

Не переводить деньги на «безопасные счета». Таких счетов не существует. Так же как не бывает «дистанционных обысков» и «декларации наличных накоплений».

Не передавать данные под давлением. Страх уголовной ответственности, обвинения в «спонсировании терроризма» или «утечке данных» — распространённая легенда.

Не выполнять «проверочные задания». Если вас просят оформить карту, скачать приложение, включить демонстрацию экрана или передать устройство курьеру — это вовлечение в преступную схему.

Примеры

1. Фейковый чат вуза и пропавший сейф

добавили в чат, который выглядел точь-в-точь как официальный канал его вуза. Там от имени «куратора» пришло срочное сообщение: нужно срочно «оцифровать личное дело» по требованию госорганов. Студент поверил — и в результате лишился своих денег и родительского сейфа.

Как работала схема мошенников: *студенту скинули ссылку на «официальный бот Госуслуг». Он перешел, ввел номер телефона, получил код и отправил его в чат — так мошенники получили доступ к его аккаунту.*

Сразу после этого ему позвонили «из полиции». Сказали: твои данные скомпрометированы, на твое имя кто-то оформил доверенность, тебя

могут привлечь к ответственности. Испуганный парень под диктовку перевел свои деньги на «безопасный счет».

Но этого показалось мало. Мошенники продолжили давить: запугали до такой степени, что студент забрал из дома родительский сейф с деньгами и передал его курьеру, который приехал по адресу.

***Какие последствия:** Семья лишилась всех сбережений. Студент остался с чувством вины и с уголовным делом, которое теперь расследует полиция. А мошенники как сквозь землю провалились.*

2. Brawl Stars и 10-летний «покупатель»

***Что произошло:** 10-летний мальчик играл в Brawl Stars и захотел купить платную подписку с бонусами. Он нашел в мессенджере канал, где продавали внутриигровые ценности «по выгодной цене». Договорился с администратором и перевел деньги. А в ответ получил блокировку.*

***Как работала схема мошенников:** ребенок сам нашел канал, сам написал администратору. Тот объяснил: чтобы пополнить «игровой кошелек», нужно просто перевести сумму на указанный номер телефона. Мальчик взял карту родителей (деньги ему выдавали на карманные расходы) и перевел. После перевода администратор сказал: «Лимит недостаточный, давай еще». Получил отказ — и просто заблокировал ребенка.*

***Какие последствия:** отец мальчика написал заявление в полицию. Деньги, скорее всего, уже не вернуть. Ребенок получил первый в жизни урок: «выгодная цена» в интернете чаще всего оказывается ловушкой.*

3. Знакомство в «Дайвинчике» и заблокированный айфон

***Что произошло:** подросток познакомился в чате знакомств с приятным собеседником. Несколько дней они общались об увлечениях, учебе, планах на жизнь. А потом новый друг попросил о помощи — и оставил парня без телефона.*

***Как работала схема мошенников:** в ходе переписки выяснилось, что у подростка iPhone. Через пару дней собеседник прислал фото разбитого телефона и расстроенный голос: «Не могу зайти в iCloud, а там важные материалы для доклада, выручи! Войди временно в мой аккаунт с твоего телефона». Доверчивый подросток ввел чужие данные на своем устройстве. Мошенник через сервис «Найти iPhone» мгновенно заблокировал телефон жертвы и вывел на экран требование выкупа — 10 тысяч рублей, иначе все данные сотрутся.*

***Какие последствия:** ребенок остался без телефона и без денег, если бы перевел. Хорошо, если родители вовремя подсказали не платить. Но осадок остался: тот, кому доверял, оказался обычным вымогателем.*

4. «Друг» по CS:GO и украденный Steam на 70 тысяч

***Что произошло:** подросток играл в Counter-Strike, нашел напарника, вместе проводили матчи, общались в Discord. Через пару недель «друг» предложил скачать альтернативный лаунчер для игры — стабильнее работает и бонусы дает. Подросток поверил и лишился аккаунта с ценными предметами.*

Как работала схема мошенников: *«друг» скинул ссылку на лаунчер и попросил войти через Steam. Ссылка вела на фишинговый сайт — точную копию официальной страницы Steam. Подросток ввел логин и пароль — доступ к аккаунту ушел мошенникам. Те сменили данные и вывели все виртуальные ценности: скины, инвентарь.*

Какие последствия: *ущерб — около 70 000 рублей (реальных денег, которые стоили эти виртуальные предметы). Аккаунт вернуть можно, но ценности — уже нет. Доверие к «друзьям из сети» подорвано.*

5. Света, Roblox и мамин онлайн-банк

Что произошло: *Света фанатела от Roblox и мечтала купить редкий скин за игровую валюту. В игровом чате написал незнакомец: «Хочешь заработать валюту? Сделай пару простых заданий». Света согласилась.*

Как работала схема мошенников: *задания оказались простыми: взять телефон мамы, открыть онлайн-банк, сделать пару кликов и переслать данные «другу». Девочка все выполнила, думая, что это игра. Ей сказали держать всё в секрете — она и держала. Мошенники через мамин телефон перевели крупную сумму себе.*

Какие последствия: *вечером мама заглянула в телефон и увидела пустой счет. Карту заблокировали, но деньги ушли. Света усвоила урок на всю жизнь: никаких «секретных заданий» от незнакомцев в чатах.*

6. Звонок из «полиции» и спасение мамы ценой денег

Что произошло: *Маше позвонили с номера, на экране высветилось «Полиция». Женский голос представился сотрудницей главка по борьбе с мошенничеством и спросил: «Горячева Валентина Михайловна вам кем приходится?» — «Мамой». — «На работе у мамы проверка, нужно срочно задекларировать имущество, иначе на нее заведут уголовное дело и посадят в тюрьму».*

Как работала схема мошенников: *ребенка напугали до ужаса: мама может сесть в тюрьму! Объяснили: чтобы спасти маму, нужно собрать все деньги и ценности, которые есть дома, и передать курьеру. Маша послушно собрала, отдала и вечером с гордостью рассказала маме, как спасла ее от тюрьмы.*

Какие последствия: *Деньги пропали. Мама поняла, что дочь обманули. Ребенок теперь знает: если звонят «из полиции» и просят деньги — это мошенники, верить нельзя.*

7. «Бабушку сбила машина» — слезы и паника

Что произошло: *Валя смотрела мультики, зазвонил телефон. В трубке — всхлипывания, похожие на плач. «Бабушка, ты?» — спросила девочка. Мужской голос ответил: бабушку сбила машина, она при смерти, нужно срочно заплатить за госпитализацию, иначе не начнут лечить.*

Как работала схема мошенников: *мошенник давил на время: «Бабушка может умереть каждую минуту! Срочно неси деньги, курьер уже едет!». Испуганная Валя открыла ящик, где лежали семейные сбережения,*

схватила сумку и выбежала к курьеру. Только вернувшись домой и немного успокоившись, она позвонила маме. Мама перезвонила бабушке — та была жива и здорова.

Какие последствия: *деньги ушли мошенникам. Ребенок в стрессе. Мама в ярости. Бабушка в недоумении. Хорошо, что хоть девочка догадалась позвонить матери, а не молчать до вечера.*

8. «Проголосуй за меня!» — ссылка от одноклассника

Что произошло: *Рома получил сообщение от одноклассника: ссылка на голосование в конкурсе. Перешел, авторизовался через соцсеть, проголосовал. Через пару часов не смог зайти в свой мессенджер — и тут же позвонил друг: «Ты просил у меня деньги в долг?»*

Как работала схема мошенников: *аккаунт одноклассника уже был взломан. С него разослали ссылку. Сайт голосования оказался фейковым. Рома ввел свои данные — и отдал мошенникам доступ к своему аккаунту. Теперь с его аккаунта рассылают просьбы о деньгах всем контактам.*

Какие последствия: *Рома потерял доступ к аккаунту. Друзья едва не перевели деньги мошенникам. Урок: даже ссылка от друга может быть опасной, если он уже взломан.*

9. Лена и «аренда аккаунта» за 2000 рублей

Что произошло: *Лена получила сообщение: «Привет! Хочешь быстро заработать?» Незнакомец предложил сдать в аренду аккаунт в мессенджере на пару дней за 2000 рублей. Девочка подумала: «Круто! Можно купить подарок маме!» — и отдала пароль.*

Как работала схема мошенников: *никакой сложной техники: просто попросили пароль и пообещали деньги за временное пользование аккаунтом. Ребенок поверил, что это реальный заработок.*

Какие последствия: *Вечером Лена похвасталась маме своей «работой» — и узнала, что теперь с ее аккаунта могут рассылать мошеннические сообщения, просить деньги у друзей, втягивать людей в схемы. Мама объяснила: «Твой аккаунт — это твое удостоверение личности. Если ты отдаешь его чужим, они могут делать что угодно от твоего имени». Лена запомнила навсегда.*