МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОФИЛАКТИКЕ АКТУАЛЬНЫХ УГРОЗ ИНТЕРНЕТ-МОШЕННИЧЕСТВА СРЕДИ РОДИТЕЛЬСКОЙ ОБЩЕСТВЕННОСТИ

Введение

В современном обществе интернет и цифровые технологии проникли практически во все сферы нашей деятельности. Мы не только совершаем банковские операции и отслеживаем покупки в режиме онлайн, но и обмениваемся важными документами через облачные хранилища, храним личные фотографии на дистанционных серверах и даже используем мобильные приложения для контроля за здоровьем и физической активностью.

Всё это кажется удобным и безопасным, однако именно повсеместность интернета может обернуться **уязвимостями**, о которых многие не задумываются. Современные мессенджеры и социальные сети стали аналогами «цифровых улиц» и «площадей», где мы проводим значительную часть времени, не всегда осознавая, что подобная открытость может привлечь злоумышленников.

Растущая популярность онлайн-игр, дистанционного обучения и телемедицины делает интернет ещё более универсальным пространством, без которого практически невозможно представить сегодняшнюю жизнь. В результате многие начинают относиться к цифровой среде как к чему-то обыденному и перестают внимательно следить за безопасностью собственных данных. Некоторые люди уверены, что преступники интересуются в основном крупными корпорациями, а обычным пользователям бояться нечего.

На практике же **жертвами** фишинга, социальной инженерии или вымогательств **становятся самые разные категории людей**. Статистика мошенничеств подтверждает, что возраст, уровень образования и социальный статус не гарантируют иммунитета от рискованных ситуаций.

В такой обстановке особенно **важно понимать, какие именно угрозы могут возникнуть при повседневной работе в интернете**. Можно иметь неплохие технические навыки, но при этом не замечать скрытых уловок мошенников, которые используют психологическое давление или обман доверия.

Личная цифровая безопасность: фундаментальные аспекты

Важным понятием, с которого стоит начать, является **цифровая грамотность**. Многие считают, что это просто умение использовать технические устройства, отправлять сообщения или

управлять банковским приложением на смартфоне. Однако цифровая грамотность гораздо шире.

Она включает в себя способность не просто пользоваться современными технологиями, но и глубоко понимать их принципы работы, **критически** оценивать поступающую информацию, а также постоянно **заботиться о защите своих личных данных** от возможных угроз.

Это умение не только своевременно обновлять программное обеспечение и правильно настраивать гаджеты, но и **вовремя распознавать опасности**, возникающие в цифровой среде. Грамотный пользователь **регулярно** расширяет и обновляет свои знания, чтобы эффективно реагировать на **стремительные изменения** в мире информационных технологий.

Другим ключевым понятием является **социальная инженерия**. Под этим термином скрывается **набор психологических приёмов**, с помощью которых мошенники пытаются повлиять на поведение людей.

В отличие от технических методов взлома, социальная инженерия направлена на то, чтобы жертва **добровольно** раскрыла конфиденциальную информацию или совершила действие, необходимое злоумышленникам.

Типичный пример — *ситуация, когда человек, испугавшись потерять деньги, сообщает мошенникам свои банковские данные, считая, что помогает «службе безопасности банка» предотвратить кражу.*

Часто **преступники могут использовать чувство жалости, доверия** или даже желание помочь, представляясь сотрудниками благотворительных фондов или друзьями, попавшими в беду. К сожалению, даже технически подкованные люди иногда становятся жертвами социальной инженерии, поскольку **эмоциональное давление** оказывает сильное воздействие и **снижает бдительность**.

Одной из наиболее распространённых угроз в цифровом пространстве является **фишинг**. Злоумышленники активно создают **поддельные сайты**, которые внешне практически не отличаются от официальных страниц банков, государственных порталов (*таких как Госуслуги*) или **популярных социальных сетей**.

Затем мошенники **рассылают ссылки на эти ресурсы** через электронную почту, SMS-сообщения или мессенджеры, заманивая пользователей различными предлогами: «проверка данных», «подтверждение транзакции» или «срочная авторизация».

Особенно опасны ситуации, когда преступники размещают такие **ссылки в рекламных объявлениях** поисковых систем. Пользователь, ничего не подозревая, переходит по ссылке, вводит личные данные, логины и пароли, после чего информация попадает в руки злоумышленников и используется в преступных целях. Кроме того, серьёзной опасностью

являются угрозы в социальных сетях и мессенджерах. **Достаточно распространённая схема** — **взлом аккаунта с целью отправки сообщений от имени настоящего владельца страницы**. В таких сообщениях мошенник может просить ваших друзей о срочной финансовой помощи, ссылаясь на экстренную ситуацию или временные финансовые трудности. Также от взломанного аккаунта часто рассылаются ссылки на вредоносные сайты или приглашения в сомнительные «закрытые сообщества».

Подобные взломы чаще всего происходят из-за использования простых или повторяющихся паролей, а также при входе в соцсети с небезопасных устройств и общедоступных сетей Wi-Fi.

Ещё один вид угроз связан с финансовыми операциями. Многие люди становятся жертвами мошенников, соглашаясь на такие схемы, как «аренда» банковских карт, передача своих SIM-карт третьим лицам, или предоставление электронных кошельков для проведения сомнительных транзакций.

Подобные предложения часто звучат очень заманчиво, особенно если человек испытывает финансовые трудности или просто хочет получить дополнительный доход. Однако на практике такие действия всегда несут юридические риски, поскольку банковские карты или SIM-карты затем используются в **незаконных схемах** по отмыванию денег или мошеннических переводах. Владелец реквизитов зачастую становится первым, к кому приходят сотрудники правоохранительных органов.

Особое внимание стоит уделить **понятию двухфакторной аутентификации** (2FA). Этот способ защиты аккаунтов становится всё более важным в условиях постоянного роста угроз информационной безопасности.

Если раньше для доступа к учётной записи было достаточно лишь одного пароля, то **сейчас этого уже недостаточно**. Двухфакторная аутентификация предполагает подтверждение личности пользователя **двумя** независимыми способами: первым является **пароль**, а вторым — дополнительный **код**, полученный через SMS-сообщение, приложение-генератор кодов или даже с помощью физического аппаратного ключа.

Такой подход значительно усложняет работу злоумышленников, ведь для успешного взлома им необходимо получить доступ сразу к нескольким устройствам или сервисам, что практически невозможно без непосредственного участия владельца аккаунта.

Понимание этих угроз и механизмов, с помощью которых мошенники пытаются манипулировать жертвами, является **обязательным для всех пользователей цифровых сервисов**. Именно осознанность и знание основных схем мошенничества помогают значительно снизить риски и защитить себя от серьёзных неприятностей.

Социальная инженерия: как мошенники используют психологические приёмы

Многие думают, что их трудно обмануть, но мошенники часто пользуются **эмоциональными «крючками»:**

- **Давление страха:** *«Если вы не сообщите код из SMS, счёт будет заблокирован»*, *«Не передадите доступ — потеряете все деньги»*. **Задача преступника** — вывести вас из состояния спокойствия, чтобы вы приняли поспешное решение.
- **Вызывание жалости или доверия:** *«Мы волонтёры, собираем на срочную операцию»*, *«Я ваш коллега, срочно помогите со служебным доступом»*. Часто используется сочувствие к больным детям или доверие к «официальным лицам». Люди, которые изначально добры и отзывчивы, могут отреагировать на подобные призывы, не перепроверяя факты.
- **Лесть и обещание выгоды:** *«Вы выиграли приз, подтвердите, введя данные карты»*, *«Участвуйте в инвест-проекте, гарантированная доходность 100%»*. Здесь делают ставку на жадность или самолюбие. Желание получить большой куш или почувствовать себя «избранным» становится причиной неосторожных действий.

Даже опытные пользователи могут попасть в ловушку, когда под эмоциями теряют **критическое мышление.**

Основная рекомендация: если вам предлагают что-то **срочно**, ссылаясь на угрозу или уникальный шанс, всегда останавливайтесь и проверяйте информацию.

Многие считают, что «в интернете никто не узнает», если они предоставят доступ к своим аккаунтам или выступят посредниками в переводах. Появляется ложное убеждение о безнаказанности, особенно если речь идёт о незнакомых людях в мессенджерах или о сделках с псевдонимами.

Некоторые пользователи верят, что раз общаются под ником, их личность остаётся в тени. Однако **правоохранительные органы обладают достаточными техническими средствами**, чтобы вычислить истинного владельца платёжного счёта или сим-карты.

Опытные пользователи нередко забывают, что их действия в сети оставляют **цифровой след**: IP-адреса, лог-файлы, привязки к определённым устройствам.

Мошенники могут воспользоваться вашей иллюзией анонимности, убеждая, что «никто ничего не узнает». На практике выясняется, что по цепочке переводов легко выйти на человека, который предоставил свою карту или аккаунт. **Незнание закона не освобождает от ответственности**, и это ключевой момент, который многие упускают.

Современные мошеннические схемы становятся всё более изощрёнными и разнообразными. Наиболее распространённым способом похищения личных данных остаётся **фишинг**. Часто пользователи получают поддельные письма якобы от официальных учреждений, банков или популярных сервисов. Такие письма, несмотря на внешнюю правдоподобность и использование официальных логотипов, при внимательном изучении обнаруживают подозрительный адрес отправителя или ошибки в тексте. Пользователь, доверившись, переходит по ссылке и вводит свои данные на фальшивом сайте, который внешне почти не отличается от настоящего. Преступники идут на хитрость, заменяя символы в адресе сайта (например, латинскую букву «l» на цифру «1»), что вводит в заблуждение даже опытных пользователей. Аналогичные схемы действуют и в виде SMS или сообщений через мессенджеры.

Например, мошенник присылает тревожное сообщение о том, что банковская карта якобы заблокирована, после чего пользователь, испугавшись, передаёт конфиденциальную информацию злоумышленникам.

Одновременно с этим набирает популярность такой вид мошенничества, как **«дропперство»**. «Дропперами» называют людей, которые предоставляют свои платёжные инструменты (*банковские карты, SIM-карты, электронные или криптовалютные кошельки*) **третьим лицам** для совершения сомнительных операций.

Часто людей привлекает возможность получить **«лёгкие деньги»**: за небольшое вознаграждение им предлагают «*всего лишь предоставить*» свои реквизиты или аккаунты.

Однако мало кто задумывается, что подобные действия трактуются законом как участие в преступлении, а точнее – **пособничество**. Многие наивно полагают, что «их никто не найдёт», ведь они «ничего не украли». Но реальность такова, что банки и правоохранительные органы легко отслеживают цепочки переводов и транзакций, поэтому даже незначительное участие в подобных схемах может привести к серьёзным последствиям, вплоть до реального **уголовного наказания**.

Особенно важно понимать, что мошенники практически всегда используют третьих лиц (дропперов), чтобы сохранить свою анонимность. В итоге реальным исполнителем, на чьё имя зарегистрированы все операции, становится тот, кто согласился передать свои данные. Нередко мошенники обещают привлекательную прибыль и «полную безопасность», однако в реальности легко оставляют своих «исполнителей» один на один с правоохранительными органами, долгами и штрафами, просто исчезая с поля зрения. Такая ситуация ставит человека в положение крайнего виновного, и доказать свою невиновность или незнание обстоятельств бывает крайне сложно. Новые законодательные инициативы стремятся ужесточить ответственность за передачу личных платёжных данных и реквизитов третьим лицам. В частности, предложенный законопроект вносит изменения в ст. 187 УК РФ («Неправомерный оборот средств платежа»), что делает наказание за

подобные действия более жёстким. В перспективе даже единичная передача карты, аккаунта или SIM-карты для мошеннических целей может обернуться крупным штрафом и даже тюремным заключением.

Государство стремится пресечь анонимный оборот денежных средств, часто используемый для финансирования преступных группировок, покупки запрещённых товаров и отмывания похищенных денег.

При этом популярные инструменты, такие как электронные и криптовалютные кошельки (**например**, Qiwi, ЮMoney или криптовалюты), вопреки распространённому мнению, **не обеспечивают абсолютной анонимности**. Несмотря на кажущуюся безопасность и конфиденциальность, **правоохранительные органы имеют возможность отслеживать транзакции** через привязку к телефонам, IP-адресам и другим цифровым следам.

Следовательно, любые операции с такими кошельками, особенно передача их третьим лицам, должны вызывать настороженность и понимание, что за незаконные действия придётся отвечать владельцу кошелька.

Алгоритмы первичной самопроверки: как распознать мошеннические предложения:

- **Кто инициировал контакт?** Если к вам обратился **незнакомец**, требующий конфиденциальных данных или предлагающий «быстрый заработок», уже есть повод насторожиться. Любые внезапные сообщения без предварительной договорённости должны вызывать вопросы.
- **Задает ли он срочность или давит на эмоции?** Фразы *«Срочно переведите, осталось 5 минут», «Никому не говорите, это конфиденциальная информация»* — типичные сигналы красного уровня. Мошенники используют эффект неожиданности.
- **Проверяйте официальные каналы.** Если вам пишут якобы из банка, перезвоните по номеру, указанному на обороте вашей карты, или на официальном сайте. **Игнорируйте телефон**, который продиктовал вам **неизвестный** человек, и **не переходите по ссылкам** из сомнительных писем.
- **Трезво оценивайте обещанную выгоду**. Любая сверхприбыль, особенно «без рисков», должна вызывать **сомнения**. Финансовые пирамиды, чудодейственные «инвестиционные фонды» и прочие быстрые схемы зачастую являются лишь прикрытием для обмана.

Технологические основы вашей защиты

Одной из **основ** цифровой безопасности является **грамотное использование паролей**. Надёжные пароли должны состоять как **минимум из 12 символов**, включая не только буквы и цифры, но и специальные знаки.

Очень важно **не использовать одинаковые пароли на разных сайтах** и сервисах, поскольку в случае утечки данных мошенники смогут получить доступ сразу ко многим вашим аккаунтам.

Старайтесь избегать паролей, содержащих общеизвестные слова, даты рождения, имена близких или другую легко угадываемую информацию. Кроме того, **рекомендуется регулярно обновлять пароли**, особенно если вы подозреваете, что ваши данные могли быть скомпрометированы.

Чтобы **безопасно и удобно хранить большое количество уникальных паролей**, стоит использовать специальные программы — **менеджеры паролей**. Эти инструменты позволяют **автоматически** подставлять пароль при входе на сайт или в приложение, избавляя пользователя от необходимости запоминать десятки сложных комбинаций.

Использование менеджеров паролей значительно **удобнее и безопаснее**, чем хранение данных в обычном текстовом файле или записной книжке. Дополнительно многие современные менеджеры могут проверять, не были ли ваши пароли скомпрометированы в результате утечки данных.

Следующим важным элементом цифровой защиты является **двухфакторная аутентификация** (2FA). Этот метод стоит включать везде, где это возможно: в банковских приложениях, социальных сетях, почтовых сервисах и других ресурсах. При двухфакторной аутентификации пользователю недостаточно знать только пароль — ему необходимо подтвердить личность дополнительным кодом, который может приходить на телефон через SMS, генерироваться специальным приложением или даже подтверждаться биометрическими данными, такими как: отпечаток пальца или распознавание лица.

Такой подход существенно усложняет задачу злоумышленникам, которым необходимо одновременно получить доступ к двум разным факторам защиты.

Также необходимым элементом обеспечения личной безопасности является **использование антивирусного программного обеспечения**. Регулярные обновления антивируса позволяют защититься от новых видов вредоносных программ, которые постоянно появляются в сети. Это особенно важно на устройствах, которыми пользуются **дети**, так как они часто скачивают приложения из непроверенных источников, переходят по ссылкам в социальных сетях или играх, рискуя подхватить вирус или вредоносное ПО.

Помимо антивируса полезным инструментом является **фаервол (брандмауэр)**, который отслеживает сетевую активность и блокирует подозрительные соединения, обеспечивая дополнительную защиту данных пользователя.

Не менее важна **регулярная проверка и контроль финансовых транзакций**. Рекомендуется подключать SMS- или push-уведомления об операциях по банковской карте и регулярно проверять историю платежей через личный кабинет банка. В случае обнаружения подозрительных или несанкционированных операций следует **незамедлительно** обращаться на горячую линию банка и

при необходимости блокировать карту или счёт. Быстрое реагирование на такие инциденты существенно повышает шансы остановить мошенников и вернуть свои деньги.

Применение этих базовых мер значительно снижает риск столкнуться с большинством цифровых угроз.

Однако, даже грамотные пользователи, соблюдающие все указанные рекомендации, иногда могут становиться жертвами более изощрённых схем обмана, в основе которых лежит не только техническая уязвимость, но и психологическое давление или недостаток правовой осведомлённости.

Именно поэтому так **важно развивать комплексный подход** к цифровой безопасности, объединяющий технические меры с постоянным повышением уровня личной осведомлённости.

Если у вас есть дети: дополнительные аспекты родительской ответственности

Школьники младшей возрастной группы (от 7 до 11 лет) также находятся в зоне повышенного риска, хотя схемы их вовлечения значительно отличаются от подростковых.

В этом возрасте дети ещё более доверчивы и менее осведомлены о рисках в интернете. У них практически отсутствует критическое отношение к информации, поступающей через гаджеты или приложения. Чаще всего они не понимают, что за аватаркой симпатичного героя из игры или дружелюбного персонажа может скрываться злоумышленник.

Особую опасность для детей младшего возраста **представляют игры** и **видеохостинги**, в которых широко распространён контент с призывами перейти по сомнительным ссылкам, получить бонусы или «подарки».

Например, ребёнок видит **рекламу**, где ему предлагают бесплатно получить *внутриигровую валюту, редкие предметы или доступ к уникальным уровням*. Для этого необходимо **«всего лишь»** ввести пароль, номер телефона **родителей** или пройти по ссылке.

Дети в таком возрасте легко поддаются на подобные уловки, потому что для них обещание награды кажется правдоподобным и безопасным. Злоумышленники осознанно ориентируются на наивность детей младшего возраста и используют яркие, красочные предложения, а также образы любимых мультгероев.

Например, ребёнок может получить сообщение в игровом чате или мессенджере от персонажа, похожего на героя популярного мультфильма, который предлагает ему обменяться аккаунтами или «поделиться» паролем для получения подарков. Младшие школьники практически никогда не

предполагают обмана в таких ситуациях, ведь у них ещё не сформирован навык распознавать подозрительные предложения.

Дети, особенно подростки в возрасте от 12 до 17 лет, активно стремятся к новым впечатлениям и самоутверждению среди сверстников. В этот период критическое мышление только формируется, и подросткам ещё трудно объективно оценивать риски и последствия своих действий. Именно поэтому они легко попадают под влияние злоумышленников в цифровом пространстве.

Мошенники осознанно ориентируются на подростков, поскольку они стремятся к **самостоятельности**, признанию сверстников и **независимости** от родителей. Интернетпреступники специально создают привлекательные предложения в социальных сетях, мессенджерах и игровых чатах, заманивая подростков обещаниями **быстрого заработка**, получения **внутриигровой валюты**, **модных вещей или дорогих гаджетов**, которых у них нет, но которые кажутся обязательным атрибутом социального статуса.

Одна из самых распространённых схем — просьба «просто» передать свой аккаунт мессенджера, страницы в соцсетях или даже доступ к банковскому приложению «на короткое время». **Взамен** подросткам **обещают вознаграждение** в виде небольших сумм или игровых бонусов.

Нередко злоумышленники начинают общение с подростком в игровой среде или группе по интересам, постепенно устанавливая дружеские отношения и доверие. Когда ребёнок расслабляется и начинает считать нового знакомого другом, просьба передать личные данные воспринимается им совершенно нормально, ведь это **«друг»**, который не может навредить.

Особенно уязвимы те, у кого дома не принято обсуждать вопросы цифровой безопасности или которые не имеют открытых, доверительных отношений с родителями.

Если ребёнок заранее уверен, что родители будут критиковать, запрещать или наказывать за любые сомнительные действия в интернете, он скорее попытается скрыть свои действия, чем обратиться за советом к взрослым.

Таким образом, недостаток коммуникации в семье делает детей ещё более подверженными влиянию мошенников, предлагающих «секретный» или «тайный» способ заработать.

Помимо прямого обмана, подростков вовлекают в мошеннические схемы с помощью давления группы. Сверстники, уже втянутые в незаконную деятельность, активно рекламируют её среди друзей, используя фразы вроде «Все так делают», «Ты же не хуже остальных», «Не будь трусом». Такая аргументация для подростка в силу возрастных особенностей оказывается убедительнее предупреждений взрослых.

Страх быть отвергнутым, высмеянным, непопулярным среди друзей оказывается для подростков сильнее, чем страх перед наказанием или последствиями закона.

Кроме того, **дети склонны недооценивать последствия своих действий**, считая, что они слишком малы, чтобы понести серьёзную ответственность, или полагая, что в интернете их невозможно отследить.

Преступники сознательно поддерживают эту иллюзию, утверждая, что «никто никогда не узнает» и «тебе ничего не грозит, ты несовершеннолетний». **На деле это не так:** правоохранительные органы легко отслеживают цепочки переводов и сообщений, а подростки, предоставившие свои аккаунты или данные, становятся участниками преступной схемы.

Таким образом, сочетание возрастных особенностей, желания социального признания, наивности, недостатка жизненного опыта и коммуникации с родителями делает подростков наиболее привлекательной и лёгкой мишенью для цифровых преступников. Именно поэтому так **важно** вовремя и доверительно обсуждать с ребёнком вопросы безопасности в интернете, чтобы снизить вероятность его вовлечения в опасные ситуации.

В Уголовном кодексе РФ предусмотрена ответственность за неисполнение обязанностей по воспитанию несовершеннолетнего (**ст. 156**). Если ребёнок систематически совершает правонарушения или участвует в преступных схемах, а родитель не принимает мер, то могут последовать **юридические последствия**.

Органам правопорядка нередко приходится сталкиваться с ситуациями, когда родители узнают о проблемах слишком **поздно**. Если обнаруживается, что подросток активно помогал мошенникам, а взрослые «закрывали глаза», встаёт вопрос об их **соучастии** или халатности.

Кроме того, при крупных ущербах или организованной мошеннической деятельности к ответственности могут привлечь и самих родителей, если будет доказано, что они были соучастниками или потворствовали этим действиям.

Например, когда родитель сознательно оформляет несколько SIM-карт и банковских карт на подростка и передаёт их третьим лицам, получая свою долю вознаграждения. Зачастую люди не задумываются, что формально становятся звеном в мошеннической цепочке.

Виды интернет-угроз, опасных для несовершеннолетних:

- **«Цепочные» предложения:** подростки массово делятся сомнительными ссылками или «флешмобами», в ходе которых нужно «достать карту родителей», «пополнить баланс» и т.п. Подросток может счесть это игрой, не понимая, что фактически участвует в цепочке рассылки мошеннических ссылок или «отмывающих» операций.

- **Вербовка через игры или чаты:** иногда «старшие товарищи» или анонимы предлагают детям «подзаработать» — создать несколько аккаунтов, предоставить SIM-карту, выступить посредником. Подростки нередко чувствуют себя польщёнными вниманием и перспективой лёгкого дохода, не думая о правовых последствиях.
- **Шантаж**: ребёнка могут **принудить** к участию в схеме, **угрожая** распространить какую-то личную информацию (взлом страницы, фото). Именно поэтому важно объяснять детям, что нельзя хранить на устройстве секретные материалы и передавать личные фото незнакомцам.
- **Как родители могут реализовать воспитательные методы для профилактики вовлечения детей в мошенничество?**

  • Открытый диалог. Обсуждайте с ребёнком реальные новости и случаи мошенничества, задавайте вопросы: *«Что ты об этом думаешь? Как можно было поступить иначе?»* **Важно** не запугивать, а сформировать критическое отношение к сомнительным предложениям.
- **Общее цифровое пространство.** Постарайтесь быть в курсе, какими приложениями и чатами пользуется подросток, **не чтобы тотально контролировать**, а чтобы понимать среду. Совместный интерес к его цифровому миру зачастую укрепляет доверие.
- **Формирование доверия**. Ребёнок должен знать, что может обратиться к родителю, если получил странное предложение, **без страха** быть высмеянным или наказанным. Если подросток боится жёсткой реакции, он предпочтёт скрыть опасный контакт.
- **Привлечение к совместной ответственности**. Предложите ребёнку выступать «цифровым экспертом» в семье: пусть помогает настраивать безопасность, обновлять ПО. Это повысит самооценку и ответственность, а также даст ему почувствовать, что родители ценят его мнение.

Отдельного внимания требует **контроль финансовых аккаунтов** и аккаунтов в социальных сетях, принадлежащих детям. Рекомендуется использовать совместный доступ к таким аккаунтам для детей **младшего и среднего возраста.**

Родители должны иметь возможность **регулярно** проверять историю финансовых операций детей, **лимитировать** суммы списаний и контролировать, **кому** ребёнок переводит деньги.

Кроме того, **полезно** настроить отдельные детские банковские карты с ограничениями на максимальные суммы операций и ежедневный лимит. Это позволит избежать значительных финансовых потерь в случае, если ребёнок станет жертвой мошенников.

В части аккаунтов социальных сетей и мессенджеров родителей также рекомендуется периодически просматривать **список друзей**, **переписку** и **группы**, в которых состоит ребёнок.

Важно делать это **открыто**, предупреждая ребёнка заранее и объясняя, что цель такого контроля — не вмешательство в личную жизнь, а его **безопасность**.

Разрешите подростку самостоятельно участвовать в процессе защиты аккаунтов, выбирая и настраивая пароли, устанавливая двухфакторную аутентификацию и изучая настройки конфиденциальности.

Кроме технологического контроля, стоит использовать инструменты **«родительского контроля»**. **Для младших детей** полезно установить программы, блокирующие доступ к нежелательному контенту.

Но **важно** не просто поставить запрет, а **объяснить** ребёнку причину таких ограничений, рассказать о возможных угрозах и опасностях. Введение разумных временных ограничений на пользование гаджетами также снижает вероятность столкновения с мошенническими предложениями и нежелательным контентом.

Подростки же требуют более деликатного подхода. Здесь более эффективен диалог, обсуждение реальных примеров мошенничества и совместное выстраивание правил поведения в сети. Если подросток понимает логику запретов и осознаёт возможные последствия, вероятность того, что он сам будет соблюдать ограничения, существенно возрастает. Важно при этом прислушиваться к обратной связи ребёнка и корректировать правила, **учитывая его мнение и опыт**. Подростки гораздо охотнее соблюдают договорённости, когда чувствуют, что их позиция учитывается и уважается.

Стратегии воспитания цифровой культуры в семье

Стратегии воспитания цифровой культуры в семье во многом базируются на понятном и прозрачном диалоге. **Первым шагом** может стать создание совместно с детьми специального **«семейного свода правил»**. Важно не просто запретить что-то делать, а чётко и спокойно объяснить, почему именно нельзя передавать третьим лицам такие данные, как пароли, PIN-коды или коды подтверждения из SMS. Дети гораздо лучше воспринимают информацию, если получают **конкретные примеры**: **например**, можно рассказать о случаях, когда кто-то из знакомых пострадал от мошенничества, потому что легкомысленно сообщил личные данные незнакомому человеку.

Также важно установить **правила реакции на подозрительные сообщения** и ситуации в сети. **Вместо того чтобы критиковать ребёнка** за «глупые вопросы», лучше заранее договориться, что в сомнительных случаях он может спокойно обратиться к родителям за консультацией, не боясь быть высмеянным или наказанным. Можно рекомендовать делать скриншоты подозрительных сообщений, чтобы вместе обсуждать их и принимать правильные решения.

Ещё одним важным аспектом является вопрос **регистрации новых аккаунтов**, особенно если при этом требуется использовать паспортные или другие личные данные. Необходимо чётко определить порядок регистрации таких учётных записей и сообщить ребёнку, что важно всегда консультироваться с родителями, чтобы не попасть в мошеннические схемы или избежать ненужных привязок к подозрительным сервисам.

Эффективной практикой для развития критического мышления детей и подростков является использование игровых и **диалоговых методов обучения**. Например, можно устраивать дома ролевые игры: *«Я — мошенник, ты — жертва, попробуй меня разоблачить»*. Во время таких игр полезно обыграть типичные мошеннические схемы, показать, какие аргументы или манипуляции могут использовать злоумышленники, и как их можно распознать.

Не менее полезно проводить дискуссии в формате *«а что будет, если…»*. В таком формате дети самостоятельно приходят к выводу, что заманчивые предложения о «лёгких деньгах» или быстрой выгоде практически всегда оказываются обманом или имеют серьёзные последствия.

Подростки могут сами приводить примеры из жизни своих сверстников или даже из школьного окружения, где уже были попытки вовлечения в сомнительные схемы. Это позволяет детям лучше понять реалистичность угроз и ощутить свою личную уязвимость перед мошенниками.

Наконец, **важнейшим принципом воспитания цифровой грамотности** является **личный пример родителей**. Если взрослые сами не придерживаются базовых правил безопасности (**например**, *передают пароли другим людям, скачивают программы с небезопасных сайтов или ведут себя неосторожно в социальных сетях*), то ребёнок будет воспринимать подобное поведение как нормальное. Принцип «делай, как я говорю, а не как я делаю» здесь работать не будет. Вместо этого стоит чаще обращаться к подростку за его мнением, вместе анализировать приложения или сайты и задавать вопросы: *«Как ты думаешь, можно ли доверять этому приложению?»*, *«Почему это безопасно или опасно?»*.

Такой подход развивает в ребёнке самостоятельность мышления и повышает его ответственность за собственную цифровую безопасность.

Алгоритмы действий при возникновении проблем

Что делать, если вы стали жертвой?

- **Немедленная блокировка**. Если заметили подозрительные списания — **заблокируйте карту**. В некоторых случаях **каждая минута может иметь значение**, так как мошенники могут моментально вывести средства.

- **Обращение в банк**. Позвоните на **горячую линию**, сообщите о факте мошенничества, оформите письменное заявление. Банки часто рекомендуют дополнительные меры, например смену логина в мобильном приложении.
- **Заявление в полицию**. Предоставьте скриншоты, распечатки, свидетельства телефонных разговоров. **Чем раньше вы заявите**, **тем выше шансы** вернуть средства или хотя бы признать вас официально потерпевшим. Не стоит затягивать с этим, иначе расследование может осложниться.
- **Смена паролей.** Если мог быть скомпрометирован ваш аккаунт в соцсетях или почте, оперативно меняйте все пароли. Лучше перестраховаться и заменить комбинации на всех критически важных ресурсах.

Если вовлечен ребёнок: пошаговое руководство для родителей

- **Сохраняйте спокойствие:** обвинения и крики только усилят скрытность подростка. Поняв, что «его отругают», он может начать удалять переписки и уничтожать важные доказательства.
- **Соберите факты:** какие аккаунты, куда переводились деньги, с кем велась переписка. Создайте копии переписки, сделайте скриншоты, чтобы при необходимости предоставить их в полицию.
- **Блокируйте опасные каналы:** заморозьте или удалите сомнительные аккаунты, карты, SIM-карты. Лучше перестраховаться и свести потенциальный ущерб к минимуму, чем потом расхлёбывать последствия.
- **Обратитесь за юридической консультацией**: чем раньше вы действуете, тем больше шансов избежать серьёзных правовых последствий. Иногда своевременное обращение может повлиять на исход дела, если докажете, что вы сами стали жертвой обмана и вовремя сообщили об этом.
- **Работайте с психологом** (*при необходимости*), чтобы помочь ребёнку пережить стресс и осознать свой поступок. **Юридический аспект** — важен, но и **эмоциональная сторона не менее значима**, особенно если подросток чувствует вину и боится дальнейших шагов.

Как понять, что ваши счета и аккаунты использовались незаконно?

- **Необычные транзакции:** приход крупных сумм от незнакомых людей, мгновенный вывод на другие счета, отсутствие внятного объяснения. Если ребёнок или кто-то из семьи **не может ясно пояснить**, откуда эти деньги, следует провести разбирательство.
- **Подозрительные SMS или push-уведомления** о переводах, которых вы не совершали. Иногда банк может заблокировать операцию или прислать уведомление, что происходит «подозрительная активность».

- **Изменения в настройках интернет-банка:** привязка новых номеров или email, неизвестные шаблоны платежей. Если вы никогда не устанавливали такие параметры, возможна компрометация.
- **Внезапная блокировка банковского аккаунта** по требованию службы безопасности. Это знак, что банк уже заподозрил что-то неладное, и вам нужно как можно скорее связаться с его представителями.

Куда обращаться за юридической и психологической помощью?

- **Полиция**. Они занимаются расследованием цифровых преступлений, могут запросить логи, IP-адреса, связаться с банками.
- **Банки** (*службы безопасности, горячие линии*). Если проблема связана с финансовыми операциями, банк — ваш первый союзник в попытке вернуть средства или заблокировать мошеннические переводы.
- **Общественные организации** (*правозащитные центры, кибердружины, «горячие линии» по интернет-безопасности*). Такие организации консультируют граждан, помогают грамотно составить заявление, в некоторых случаях обеспечивают бесплатную юридическую поддержку.
- **Психологические службы** (*государственные и частные*) — при необходимости работы с травмой или профилактики повторного вовлечения. Иногда стресс от обмана или угроз может сильно сказаться на эмоциональном состоянии, и профессиональная помощь окажется незаменимой.

«Методические рекомендации АНО «Агентство поддержки государственных инициатив» (разработаны при поддержке ФСБ России)».

Ссылка на оригинал: https://www.единыйурок.рф/internet.