МОШЕЛОВКА.РФ

Как сделать интернет безопасным для ребенка

**Общение в интернете, онлайн-игры и бесконечный видеоконтент — как быть уверенным, что ребенку не грозит опасность в сети?
Объясняем, как научить детей правильному использованию гаджетов.**

- ✓ Поставьте на все устройства антивирусное решение, обеспечивающее защиту от вредоносных программ и вирусов.
  По результатам исследования «Лаборатории Касперского», это делают только 25% родителей.
- ✓ Устанавливайте на телефон или планшет только приложения из официальных источников, причем с максимально широким функционалом и гибкими настройками.
- ✓ Используйте программу отслеживания местонахождения ребенка в режиме реального времени, особенно если между школой, секциями и домом он передвигается в одиночку.
- ✓ Выстраивайте с детьми доверительные отношения, чтобы они всегда знали, что могут обратиться к вам.
- ✓ Проводите качественно и интересно время с ребенком в реальной жизни.
- ✓ Помогайте ему развивать уважение к другим людям, критическое мышление и эмоциональный интеллект.
  Среди опрошенных родителей 48% обсуждают с детьми правила поведения в сети.
- ✓ Будьте в курсе, какие приложение, игры и социальные сети ребенок скачивает и использует. Убедитесь, что они соответствуют его возрасту. Проверьте в них настройки конфиденциальности.
- ✓ Следите, чтобы дети не размещали в социальных сетях персональную информацию о себе и семье.
  Интересно: 50% школьников указывают в сети настоящий возраст или делятся своими фотографиями.
- ✓ Используйте родительский контроль.
  Только 21% родителей школьников установили такие программы.
- ✓ Установите ограничения по времени пользования гаджетами.
  Сейчас этому правилу следует 31% родителей.
- ✓ Обращайте внимание на поведение и настроение ребенка: любое изменение может говорить о том, что он попал в сложную ситуацию. Согласно опросам, 47% детей скрывают от родителей, чем они занимаются в интернете.

Обратите внимание, что сначала следует научить ребенка перемещаться в онлайн-пространстве с помощью родительского контроля и специальных семейных настроек в сервисах, к которым у него есть доступ. По мере взросления и погружения в виртуальную реальность технические меры будут постепенно отходить на второй план, а на первое место выйдет обучение и повышение цифровой грамотности подросших пользователей.

Мошенники стали вчетверо чаще звонить от имени сотовых операторов

Мошенники стали чаще звонить от имени сотовых операторов с требованием продлить SIM-карту. По данным приложения Kaspersky Who Calls, число таких звонков в октябре по сравнению с сентябрем выросло втрое, а в ноябре (по сравнению с сентябрем) — уже вчетверо.

На платформе Народного фронта «Мошеловка» подтвердили всплеск: легенду со звонками от имени сотовых операторов начали фиксировать с конца лета, но уже сейчас она попал в топ наиболее используемых злоумышленниками.

«Схема выглядит так: человеку звонит мошенник, представляется сотрудником телеком-оператора и сообщает, что срок действия SIM-карты или договора на предоставление услуг связи заканчивается. При этом в личном кабинете информация якобы не отображается, поэтому уведомление происходит в устной форме», — рассказал главный эксперт «Лаборатории Касперского» Сергей Голованов.

Он пояснил: звонящие пытаются выманить конфиденциальные и учетные данные от личного кабинета абонента, а также одноразовые коды. Если злоумышленники их получат, то попытаются установить переадресацию СМС на нужный им номер или выпустить виртуальный дубликат SIM карты (eSIM).

Таким образом преступники смогут добраться до личного кабинета пользователя в других сервисах, в том числе финансовых и информационных.

Как обманывают мошенники (распространенные приемы мошенничества)

Телефонные мошенники

Приемы:

- Представляются сотрудниками банка и пугают потерей средств.
- Заводят разговор о переводе денег (оплата штрафов, налогов, услуг).
- Заставляют взять кредит.
- Просят сообщить реквизиты банковской карты (ее номер, CVV/CVC-код).
- Просят продиктовать одноразовый код из SMS.
- Просят установить приложение на телефон “для защиты средств”.
- Просят срочно перевести деньги на “спасение” близких.

Что делать, если у вас списали деньги:

1. Обратиться в банк и заблокировать счет.
2. Потребовать отменить транзакцию в банке немедленно: некоторые платежи можно успеть вернуть.
3. Потребовать от банка провести чарджбек (оспаривание платежа, с которым вы не согласны). Условия процедуры зависят от политики банка и платежных систем.
4. Обратиться в полицию с заявлением и требованием возбудить уголовное дело.
5. Если в возбуждении дела полиция отказала, можно это оспорить в прокуратуре или суде.

Кибермошенники

Приемы:

- Создают подменные сайты, замаскированные под официальные ресурсы компаний (страховая, банк, госучреждение). С помощью них собирают все доступные данные, включая реквизиты карт и счетов (фишинг).
- Распространяют вирусное ПО, которое позволяет автоматически переадресовывать вас на поддельные сайты, где похищают данные (фарминг).
- Взламывают аккаунты ваших друзей и близких в социальных сетях и мессенджерах, просят “в долг” от их имени.
- Представляются несуществующими благотворительными организациями и просят помочь “больным детям”.

Что делать, если у вас списали деньги:

1. Подать заявление в полицию.
2. Если списали деньги без вашего ведома, немедленно обратитесь в банк: заблокируйте счет и постарайтесь оспорить транзакцию.
3. Направьте обращение в департамент по недобросовестным практикам Банка России.

Взяли кредит на ваше имя

Признаки

- Звонят / пишут с неизвестных номеров и требуют погасить долг.
- Угрожают расправой вам и вашим близким, если не вернете кредит.

Если никаких займов вы не оформляли, то:

1. Выясните, откуда у мошенников ваши паспортные данные. Если вы потеряли паспорт, немедленно сообщите в полицию и возьмите справку об утере паспорта с указанием даты.
2. Закажите справку в Бюро кредитных историй и узнайте, реально ли у вас есть задолженность – это бесплатно 2 раза в год. Узнать, в каких БКИ есть ваша кредитная история, можно на Госуслугах.
3. Если за вами числятся кредиты, которые вы не брали, обратитесь к кредитору с требованием ликвидировать долг и обратитесь в БКИ для проведения проверки.
4. Выясните подробности сделки: запросите у кредитора заверенные копии договора и удостоверения личности заемщика, данные сотрудника и адрес офиса, где оформляли договор. Соберите максимум данных и подайте заявление в полицию.
5. Напишите жалобу в Банк России.
6. Если проблему решить не удается, обратитесь в суд и ходатайствуйте о проведении экспертизы документов и подписей.

Псевдолизинг

Приемы

- **Изначально предлагают взять кредит под залог автомобиля или квартиры.**
- Выдают себя за ломбарды, банки или МФО, имеют официальные сайты.
- Представляют фирму-однодневку.
- Создают суету, не дают внимательно прочитать договор.
- Оформляют договор купли-продажи по заниженной стоимости, при этом завышают стоимость неустоек и штрафов.

Что делать:

1. Выясните все о лизингодателе: сайт, регистрационные данные, наличие сведений в перечнях Банка России.
2. Направьте претензию лизингодателю.
3. Направьте обращение в Банк России о факте нелегальной деятельности.
4. Направьте обращения в МВД РФ и в прокуратуру.
5. Обратитесь в суд с иском о признании данной сделки недействительной.

Инвестиции

Признаки:

- Не имеет лицензии на привлечение средств граждан.
- На сайте нет информации о собственных активах и финансовом положении.
- Слишком высокая заявленная прибыльность.
- Нет гарантии, что прибыль выплачивается от дохода организации, а не от других участников.
- Просят привлекать знакомых, чтобы получать выплаты.
- В договоре отсутствует ответственность перед инвестором.
- Нет информации об учредителях и владельцах.

Что делать:

1. Проверьте наличие данных об организации в ЕГРЮЛ и на сайте Банка России.

2. Направьте претензию в эту организацию с указанием доводов, требований и последствий их неисполнения.
3. Направьте обращение в Банк России.
4. Обратитесь в МВД РФ и прокуратуру.

Черные кредиторы

Признаки:

- Нет разрешения Банка России на выдачу кредитов (отсутствие в государственном реестре Банка России).
- Не требуют дополнительных документов (“быстрые деньги”).
- Займодатель – неизвестное вам лицо (ИП, физлицо или ООО, которое не соответствует названию с вывески).
- Слишком высокий % по кредиту.
- Предлагают “выгодные” условия под залог имущества.
- Жесткие методы работы с должником (запугивание, угрозы, в том числе в сторону родственников).
- Требуют деньги до выдачи кредита (например, на страховку, за перевод на счет и т.п.).

Что делать:

1. Соберите всю информацию об организации-кредиторе, указанную на сайте Банка России, в ЕГРЮЛ, в договоре.
2. Обратитесь в Банк России.
3. Обратитесь в полицию и прокуратуру.

Псевдоброкеры

Признаки

- Нет лицензии на операции с привлечением чужих средств.
- Нет информации об организации или она не зарегистрирована в РФ.
- “Гарантирована” высокая прибыльность в короткие сроки.
- Навязывают услуги по телефону — звонят с неизвестных, скрытых номеров.

Что делать:

1. Соберите всю информацию об организации в ЕГРЮЛ и на сайте Банка России.
2. Направьте претензию в эту организацию с указанием доводов, требований и последствий их неисполнения.
3. Направьте обращение в Банк России.
4. Обратитесь в МВД РФ и прокуратуру.

Философия безопасности

Сохранить свои деньги поможет свод правил безопасного поведения в сети.

1. Не делитесь личными данными, номерами карт, а тем более не переводите средства на подозрительных сайтах, малознакомым людям.
2. Никому не сообщайте коды из СМС.
3. Не принимайте поспешных решений.
4. Критически оценивайте любое финансовое предложение, максимально выясняя все подробности.
5. Заподозрив обман, сразу прекращайте беседу.

Если мошенникам все же удалось лишить вас средств, сразу действуйте:

- При наличии переписки скопируйте все диалоги со злоумышленниками.
- При потере данных банковской карты заблокируйте ее.
- Возьмите выписку в банке о передвижении ваших средств.
- Подайте заявление в полицию, приложив при наличии аудиозапись разговоров.
- Оформите жалобу на аккаунт мошенников в социальной сети или обратитесь в поисковую систему с просьбой заблокировать страницу поддельного сайта.

Чем может быть полезна аудиозапись телефонного разговора

Сервисы по записи телефонных разговоров – современная «записная книжка», которая позволяет обходиться без ручки и блокнота во время беседы по телефону. Кроме очевидных плюсов, программа может зафиксировать содержание нежелательных звонков от мошенников. Если вы пострадали от действий телефонных аферистов или сразу раскусили их, подавайте заявление в полицию и обязательно приложите запись разговора. Она поможет найти и остановить преступников.

Встроенная функция

Некоторые телефоны на платформе Android изначально обладают функцией записи. Чтобы проверить, есть ли она в вашем устройстве, зайдите в раздел телефонных звонков, перейдите в «Настройки», затем поищите «Запись звонков» или похожую строку. Если нашли, осталось только настроить разрешения.

На телефоны, у которых нет такой возможности, можно установить специальную программу. Их множество: бесплатные, платные, для Android и для iOS. Расскажем о некоторых из них.

Для смартфонов на платформе Android

Talker ACR. По словам разработчиков, бесплатное приложение поможет записывать входящие и исходящие звонки не только через телефон, но и мессенджеры и даже социальную сеть. Отличается качественным звуком. Предполагает поддержку вашим смартфоном записи вызовов VoIP (технология преобразования обычного речевого сигнала в цифровой поток для передачи в интернет).

Премиум-версия отличается дополнительными возможностями копирования записи на карту или в облако, управлением файлами, дополнительной защитой и расширенным спектром аудиоформатов, возможностью пометки важных моментов и быстрого их поиска при прослушивании разговора. Диапазон расценок на платный контент колеблется от 120 до 650 рублей.

Cube ACR. В бесплатном приложении заявлены такие функции, как запись входящих и исходящих телефонных разговоров, а также VoIP-разговоров в мессенджерах, выбор контактов для регулярной записи или их исключения, выбор

динамиков для комфортного режима прослушивания. Премиум-подписка отличается возможностью резервного копирования в облако, дополнительной степенью защиты, расширенным списком форматов аудиофайлов, скачиванием на телефон, выделением пометок в разговоре для и быстрого поиска при прослушивании, управлением записями. Заявлен платный контент от 89 до 500 рублей.

Для смартфонов на платформе iOS

Recostar. Приложение записывает исходящие и входящие звонки, загружает их в формате HD, хранит на устройстве, в облаке. Есть возможность пересылки записей по почте, в мессенджерах или в социальной сети. Сервис в магазине заявлен как бесплатный со встроенными покупками, но, если вчитаться в его описание, становится ясно, что чек ежемесячной оплаты мобильному оператору скорее всего вырастет. Одновременно с обычным звонком будет идти второй – на номер доступа к платформе записи разговоров. Это так называемая «трехсторонняя связь» или конференц-связь, за которую придется доплачивать, если ваш тариф не предусматривает бесплатного использования данной услуги. При ближайшем знакомстве с ответами разработчиков на оценки и отзывы регулярно встречается фраза «приложение является платным». Стоимость подписок – от 199 за неделю до 699 рублей за год.

REKK Запись звонков. Среди функций приложения указаны запись входящих и исходящих звонков, их конвертация в текст, возможность делать заметки к аудиозаписям, резервные копии к файлам. Пользователи могут делиться ими в мессенджерах, держать в облачных хранилищах, создавать ссылки к ним. Разработчики заявляют об удобном поиске записи по номеру, имени и тексту. Приложение заявлено как бесплатное со встроенными покупками, однако в ответах разработчиков на вопросы пользователей можно убедиться, что сервис все же является платным. Стоимость тарифов колеблется от 199 до 1790 рублей.

Прежде чем устанавливать любую из программ, внимательно ознакомьтесь с условиями разработчиков, технической совместимостью с версией операционной системы вашего смартфона и дополнительными функциями, которые потребуются от сотового оператора (за отдельную плату!) – информация об этом размещена на странице приложения. Не лишним станет почитать часто задаваемые вопросы пользователей и ответы на них.

Сервисы от мобильных операторов

Тинькофф Мобайл предлагает абонентам на территории РФ сервис по записи и расшифровке текущих разговоров, которые хранятся в приложении оператора или на сайте в личном кабинете в течение шести месяцев. Диалоги можно скачать на телефон в виде аудиофайла или текста, отправить по почте, в СМС или мессенджере.

В Тинькофф Мобайл утверждают, что сервис может служить доказательством общения с аферистами и помочь клиенту и банку в расследовании случаев мошенничества. Например, когда обманывают по сценарию с псевдоинвестициями или покупкой и продажей товаров. По словам оператора, банковская технология может выступить гарантом того, что запись не смонтирована и не подделана.

«У нас был случай, когда мошенник взломал аккаунт пользователя популярного сайта для бронирования отелей. Наш сотрудник думал, что общается с хозяином гостиницы, а на самом деле это был мошенник. После того, как деньги были переведены, выяснилось, что его обманули. Записи звонков, которые пострадавший отправил в службу поддержки сайта, помогли оперативно разобраться в ситуации и вернуть средства. Запись звонков может быть полезна для расследования других преступлений: шантажа, вымогательства, прямых угроз», – поделились в Тинькофф.

Абоненты **МегаФон** могут воспользоваться подобной услугой с помощью приложения оператора eMotion, которое подходит как для Android, так и для iPhone. Оплата за сервис осуществляется в рамках привычного тарифа независимо от региона.
Чтобы сделать запись звонков абонентам **МТС,** понадобится сервис «Мой Коннект», который можно установить и на телефоны с ОС Android, и iOS. Интересно, что при наличии интернета его можно использовать вместо оплаченного тарифа с целью экономии минут в домашнем регионе и за его пределами. Список территорий, где не работает сервис, доступен на сайте оператора.
Билайн и Теле2 предлагают такую услугу только корпоративным клиентам**,** а **оператор Yota** пока не обзавелся подобным сервисом**.**

На что подписались

Всем, кто пользуется приложениями операторов, сторонними сервисами, простыми диктофонами, нажимая на кнопку записи, нужно знать, что голос – это личные биометрические данные, поэтому здесь в силу вступает закон об ограничении на обработку и распространение подобной информации. Перед нажатием REC нужно

предупредить о своем намерении записать разговор и впоследствии использовать информацию исключительно в личных целях, как заметку, не выкладывая в открытые источники. С этими условиями вы автоматически соглашаетесь, подключая сервис у мобильных операторов.

Стоит иметь в виду, что за сохранность и конфиденциальность информации, полученной данным способом, они ответственности не несут. И в случае попадания вашего устройства к третьим лицам вся ответственность за возможное распространение таких данных будет лежать на вас.

Что говорит закон

Телефонные аферисты в разговоре никогда не выдают ни свои персональные данные, ни коммерческие тайны, ни сведения об их частной жизни, поэтому передача записи диалога с ними в полицию не нарушает законодательство РФ.

Важно, чтобы на момент написания заявления аудиозапись разговора находилась в телефоне, тогда ее изъятие смогут оформить по всем правилам и приложить к документу. Это будет являться подтверждением, что файл не подвергся изменениям в чьих-либо интересах.

Если вы или ваши близкие смогли повлиять на ситуацию с помощью записи разговоров с мошенниками, пожалуйста, поделитесь своей историей. Это станет инструкцией к действию тем, кто будет нуждаться в защите своих интересов.