Какие правила кибербезопасности надо знать школьнику

Школьный период — важный и ответственный этап в жизни каждого человека. Дети постоянно сталкиваются с новыми вызовами. Использование школьниками смартфонов и цифровых сервисов — это удобство и необходимость, которые сопряжены с киберрисками.

Интернет полон скрытых угроз для ребёнка: мошенничество, кибербуллинг, нежелательный контент и многое другое. Важно не только купить гаджет школьнику, но и подготовить его к правильному и безопасному использованию устройства. Родители должны оградить детей от неприятных ситуаций и научить правильно реагировать на потенциальные опасности в цифровом мире.

Когда ребёнок получает смартфон, важно уделить внимание настройкам устройства и ключевым аспектам кибербезопасности. Рассмотрим основные шаги, которые помогут вам познакомить ребёнка с возможными киберрисками и объяснить, как вести себя в сомнительных ситуациях.

Сервисы родительского контроля

Родительский контроль — это первое, о чём следует позаботиться. Он позволяет ограничить доступ ребёнка к нежелательному контенту, управлять временем использования устройства и контролировать загрузку приложений.

Большинство современных смартфонов имеют встроенные функции родительского контроля. Для iOS это «Экранное время» + «Локатор», для Android — Google Family Link, который предоставляет аналогичные возможности. Эти инструменты позволяют ограничить доступ к определённым сайтам, установить временные рамки использования приложений и контролировать процесс скачивания программ.

Можно рассмотреть установку специализированных приложений, таких как Kaspersky Safe Kids. Они предоставляют расширенные возможности мониторинга и управления, включая отслеживание местоположения ребёнка, фильтрацию контента и контроль за активностью в интернете.

Ограничение доступа к контенту и нежелательным покупкам

Встроенные возможности родительского контроля позволяют установить возрастные ограничения на приложения и контент, а также блокировать доступ к определённым нежелательным сайтам и контролировать активность в интернете. Научите ребёнка разумно распределять время между учебой, отдыхом и развлечениями. Используйте функции родительского контроля, чтобы установить ограничения на время использования приложений и интернета. Важно побуждать ребёнка к занятиям спортом, чтению книг и очному общению с друзьями. Это помогает сохранить баланс между цифровой и реальной жизнью.

Чтобы избежать нежелательных расходов, отключите возможность совершать покупки в приложениях без вашего разрешения и настройте оповещения о каждой такой попытке. Устройства на базе iOS позволяют оплачивать покупки с баланса мобильного оператора, эту функцию тоже стоит ограничить.

Контроль геопозиции

Встроенные функции «Найти iPhone» или Google Find My Device позволяют вам в любой момент узнать, где находится ваш ребёнок. Это особенно полезно в экстренных ситуациях. Программы с функцией родительского контроля дают возможность следить за перемещениями в режиме реального времени. Вы можете настроить уведомления о прибытии или уходе ребёнка из школы или дома.

Обратите внимание на приложения, которые запрашивают доступ к геолокации. Давайте разрешение только тем, которые действительно в этом нуждаются. В иных случаях стоит ограничить приложениям доступ к информации о местоположении.

Защита личных данных на смартфоне

Обеспечение безопасности личных данных ребёнка — важная задача для родителей. Если устройство поддерживает функции биометрической аутентификации, такие как распознавание лица или отпечатка пальца, активируйте их. Это добавит дополнительный уровень защиты.

Важный шаг в защите личных данных на смартфоне — создание надёжных паролей для доступа к различным ресурсам. Научите ребёнка, что пароли должны состоять из букв разного регистра, цифр и специальных символов. Пусть не применяет простые и легко угадываемые пароли, такие как

«1234» или даты рождения. Можно использовать специальные приложения LastPass, 1Password, Kaspersky Password Manager или аналогичные сервисы, которые помогут сохранять и генерировать сложные пароли.

Убедитесь, что на устройствах ребёнка установлены актуальные антивирусные программы. Объясните, зачем они нужны и как защищают устройство. Расскажите о важности своевременного обновления приложений и операционной системы. Это защитит от уязвимостей, которые могут быть использованы злоумышленниками.

Родителям также важно настроить автоматическое резервное копирование данных на смартфоне ребёнка, чтобы в случае утери или кражи устройства информацию можно было восстановить. Это можно сделать через встроенные облачные сервисы, такие как iCloud для iPhone или Google Drive для Android.

Защита от поддельных ссылок и сайтов

Одним из самых распространённых методов мошенничества в интернете является рассылка подозрительных ссылок. Ребёнок должен научиться избегать этих ловушек. Объясните, что если он получает ссылку в сообщении от незнакомого человека, то ни в коем случае не следует по ней переходить. Но даже если сообщение выглядит правдоподобно или приходит от знакомого человека, всегда лучше перепроверить информацию у родителей. Злоумышленники могут использовать взломанные аккаунты для рассылки вредоносных ссылок.

Расскажите о том, что мошенники с целью получения личных данныхмогут создавать сайты, очень похожие на настоящие. Ребёнок должен понимать, чтонельзя вводить личную информацию на подозрительных сайтах. В подобных случаях следует проконсультироваться с родителями.

Безопасность в онлайн-играх

Онлайн-игры — это потенциальный источник опасностей, особенно если в них участвуют незнакомые люди, чьи намерения не известны. Объясните ребёнку, что не следует общаться с незнакомцами в играх, особенно если они предлагают что-то купить или поделиться личной информацией. Ребёнок должен понимать, что его данные могут быть использованы в целях мошенничества.

В некоторых играх можно встретить предложения о покупке игровых предметов за реальные деньги. Объясните ребёнку, что подобные действия могут привести к непредвиденным расходам, а также стать ловушкой мошенников. Всегда лучше посоветоваться с родителями перед тем, как что-то покупать в игре.

Безопасность в соцсетях

Социальные сети — это платформы для общения и самовыражения. Но если не соблюдать правила безопасности — могут возникнуть проблемы. Помогите ребёнку настроить приватную учётную запись в соцсети. Пусть его сообщения, фото и видео видят только те люди, которых он добавил в друзья. Также объясните, как блокировать пользователей, которые ведут себя агрессивно или некорректно.

Научите ребёнка не публиковать в социальных сетях личную информацию, такую как адрес, номер телефона, номер школы, данные о местоположении. Эти данные могут быть использованы злоумышленниками. Научите ребёнка думать о последствиях своих действий в интернете, особенно в социальных сетях. Все комментарии, публикации и лайки формируют его цифровую репутацию, которая может повлиять на его будущее.

Некоторые вирусные челленджи могут быть опасными для здоровья и жизни. Ребёнок должен понимать, что участвовать в подобных акциях без одобрения родителей нельзя. Объясните ему, что не всё популярное в соцсетях безопасно.

Групповые чаты в мессенджерах: как избежать угроз

Мессенджеры часто используются для общения в группах. Это удобно, но может быть опасно, если не соблюдать осторожность. Объясните ребёнку, что его могут добавлять в группы незнакомые люди, и это — риск. Научите, как через меню настроек покинуть группу, если не хочется больше там находиться.

В группах могут отправлять подозрительные ссылки и файлы. Объясните школьнику, что не следует открывать файлы и переходить по ссылкам, если он не уверен в их безопасности. Если возникают сомнения — лучше спросить родителей.

Кибербуллинг и кибергруминг

Кибербуллинг — это ещё одна серьезная угроза, с которой может столкнуться школьник в интернете. Важно, чтобы он знал, как защитить себя. Объясните, что на агрессивные или оскорбительные сообщения лучше не отвечать. Вместо этого надо сохранить доказательства (скриншоты) и сразу сообщить о проблеме вам или учителю. Научите ребёнка блокировать обидчиков и сообщать о них администрации платформы или мессенджера. Это поможет прекратить агрессивное поведение.

Кибергруминг — это процесс, при котором злоумышленники через интернет устанавливают доверительные отношения с ребёнком для дальнейшего манипулирования и сексуальной эксплуатации. Очень важно, чтобы ребёнок понимал, что не все люди в интернете — друзья. Даже если они кажутся дружелюбными, присылают подарки и предлагают встретиться в реальной жизни.

Защита данных банковских карт

Если у ребёнка есть собственная банковская карта или доступ к вашим средствам, важно научить его безопасному обращению с финансовыми инструментами в интернете. Расскажите, что нельзя вводить данные банковской карты на подозрительных сайтах и передавать информацию о карте третьим лицам. Объясните, что покупать что-то в интернете можно только с вашего разрешения. Настройте уведомления о транзакциях, чтобы вы всегда знали о покупках ребёнка.

Объясните ребёнку, что если кто-то просит у него деньги или данные карты, говорит, что ошибочно перевёл деньги и просит вернуть их — это почти всегда мошенничество. Даже если кажется, что человек нуждается в помощи, лучше проконсультироваться с родителями.

Дропы и предложение лёгкого заработка в интернете

Дроп — это подставное лицо, участвующее в схеме мошенничества с «отмыванием» и обналичиванием переведённых обманутыми гражданами денег. Мошенники обычно привлекают детей и подростков обещаниями лёгкого и быстрого заработка, не раскрывая истинную суть операций. Например, ребёнку могут предложить «продать» свою банковскую карту или принять перевод и затем отправить деньги дальше.

Эти деньги обычно украдены и переводятся на другие счета, часто за границу, что затрудняет их отслеживание. В результате ребёнок, сам того не осознавая, становится соучастником преступления, имеющего серьёзные правовые последствия.

Интернет пестрит предложениями лёгкого заработка: работа «курьером» или «переводчиком» денег, игры-кликеры для «майнинга криптовалют» или получения реальных денег, огромные прибыли за привлечение новых участников и др. Объясните ребёнку, что такие предложения связаны с обманом и могут привести к серьёзным проблемам: от потери личных данных и денег до уголовной ответственности (в зависимости от возраста ребёнка).

Распознавание ложной информации (фейков)

Дети должны уметь отличать правду от фейков. Объясните ребёнку, что не вся информация в интернете является достоверной. Научите его проверять источники информации и не верить всему, что он видит в социальных сетях или на сайтах.

Современные дипфейки могут выглядеть правдоподобными, и даже взрослым бывает сложно распознать подделку. Мошенники могут использовать дипфейки, чтобы обманом заставлять передать деньги или информацию. Поэтому дети должны быть внимательны к контенту в интернете. Школьники не всегда понимают разницу между нативными рекламными материалами и личным опытом других людей в сети. Помогите ребёнку осознать, что многие блогеры и знаменитости продвигают продукты за деньги, и это не всегда означает, что эти продукты хорошие или безопасные и стоят столько, сколько за них просят.

Подготовка к экстренным ситуациям

Иногда школьник может столкнуться с ситуациями, которые вызывают у него сомнения или страх. Важно, чтобы он знал, как реагировать в таких случаях. Объясните ребёнку, что если он получает странные сообщения, видит что-то неприятное или сталкивается с подозрительными людьми

в интернете, он должен сразу рассказать вам об этом. Вы всегда готовы помочь, и он не должен бояться обращаться к вам за советом.

Но даже при всех мерах предосторожности важно подготовиться к возможным чрезвычайным ситуациям. На устройстве можно настроить быстрый доступ к экстренным контактам, которые ребёнок сможет вызвать при необходимости. Это могут быть контакты родителей, близких родственников или служб спасения.

Объясните ребёнку, что делать, если смартфон потерян или украден. Убедитесь, что он знает, как сообщить вам о происшествии. Научите ребёнка не паниковать, если он случайно перешёл по подозрительной ссылке или получил сообщение сомнительного содержания.

Родители играют ключевую роль в формировании у детей навыков безопасного использования современных технологий. Подготовка ребёнка к школе — это не только покупка учебников и школьных принадлежностей. В условиях растущей зависимости от технологий и интернета важно, чтобы ребёнок знал, как правильно использовать свой смартфон и какие угрозы могут подстерегать его в сети. Обеспечьте школьника не только техническими средствами защиты, но и знаниями об опасностях в интернете. Научите критически оценивать информацию, быть осторожным и сообщать вам о любых сомнительных ситуациях. Важно, чтобы ребёнок понимал, что его безопасность и благополучие важнее всего, и вы всегда готовы поддержать его. Создайте атмосферу доверия, в которой ребёнок не побоится обратиться к вам за помощью или советом.