ЧЕК лист к занятию ЦППР

Ақпараттан ақ-қараны ажырату өнері.

Ребенок в интернете: как найти золотую середину

Как обезопасить детей в интернете: инструкция для родителей

По данным Data Reportal, в Казахстане уровень проникновения интернета в начале 2024 года составил 92.3%. Также в стране было подключено в общей сложности 26,24 миллиона абонентов сотовой связи, что эквивалентно 133,1 процента от общей численности населения. Это значит, что интернет для многих казахстанцев является каждодневным инструментом для связи, работы, получения информации, услуг и так далее.

К тому же, пользователями интернета и девайсов являются не только взрослые, но и дети. Поэтому безопасность детей в Сети так же важна, как и безопасность офлайн. При этом безопасность детей в интернете — относительно новая тема для многих.

Сегодня существует много инструкций о том, что делать родителям, чтобы защитить своих детей в Сети. И первая из них — учить ребёнка безопасно пользоваться интернетом. Гайды от ЮНИСЕФ, Internet Matters (рекомендации поделены на возрастные группы), CloudWards могут в этом помочь.

Команда проекта «Дети&Сети», опираясь на вышеуказанные и другие источники, собрала рекомендации, которые помогут родителям создать безопасное пространство в интернете для детей.

Угрозы и решения

Рассмотрим, с какими угрозами могут столкнуться дети в Сети, и как можно с ними справиться.

Кликджекинг (clickjacking)

Кликджекинг — это метод, при котором злоумышленники маскируют ссылки или кнопки, заставляя пользователей выполнять действия, о которых они не подозревают. Например, кнопка «Нажми здесь, чтобы получить бесплатный iPhone!» может привести на нежелательную страницу и, потенциально, потере персональных данных или даже финансовых средств.

Важно объяснять детям, что такие предложения часто являются обманом.

С другой стороны, бывает, что дети случайно совершают покупки в лицензированной онлайн игре, где за дополнительные деньги игрок может получить бонусы и улучшения. Настройки аккаунта на устройствах, такие как запрет онлайн-платежей, помогают избежать такой ситуации. Помимо этого:

Регулярно проверяйте, какие приложения установлены на устройстве.

Договоритесь с ребёнком, что вы будете скачивать новые игры вместе.

Расскажите, как распознать попытку взимания денег, например, переход в магазин приложений.

Дети часто оказываются уязвимым звеном, которым могут воспользоваться мошенники для перевода денег, кражи данных и других незаконных действий. Поэтому родителям не стоит давать ребёнку свои личные устройства (телефон, планшет и т.д.), на которых содержится чувствительная информация. Лучше запастись ещё одним запасным девайсом или, если ребёнок достаточно взрослый, приобрести ему собственный.

Вредоносное ПО (malware)

Вредоносное ПО — программное обеспечение, которое при установке может повредить устройство, следить за ребёнком и ее/его окружением или похитить персональные данные. Вредоносное ПО может проникнуть на устройство через скачивание файлов из ненадежных источников, клики на подозрительные ссылки, открытие вложений от неизвестных отправителей. Но иногда это может произойти из-за уязвимости устройства или приложений, без активного действия со стороны пользователя (zero-click). Чтобы избежать этого:

Объясните детям, что нельзя скачивать файлы с неизвестных сайтов.

Регулярно обновляйте программное обеспечение и приложения и убедитесь, что устройство защищено антивирусом.

Фишинг (phishing)

Фишинг — это попытка обманом получить личную информацию, например, пароли или данные кредитных карт через письма или сообщения, которые имитируют официальные, либо через ложные сайты, похожие на настоящие.

Чтобы не попасться на фишинг, важно научить детей не вводить личную информацию на незнакомых сайтах и не переходить по подозрительным ссылкам. В зависимости от возраста ребёнка, родители могут взять на себя ответственность за проверку его почты и мессенджеров на предмет подозрительных писем и сообщений.

Кибербуллинг (cyberbullying)

Кибербуллинг — травля и издевательства в Сети. Кибербуллинг может включать негативные комментарии в социальных сетях, публикацию или распространение унизительных фото, угрозы и преследования в сообщениях.

Один из действенных способов избежать кибербуллинга — настроить приватность аккаунтов в соцсетях. Сегодня онлайн-платформы уделяют большое внимание борьбе с травлей в интернете. Поэтому автоматические алгоритмы могут также сами находить и блокировать контент, содержащий кибербуллинг. Вместе с тем у соцсетей имеются функций подачи жалобы, а также центры безопасности.

Помимо технических аспектов, есть и психологический — важно наличие доверительных отношений с ребёнком, чтобы ей/ему было комфортно делиться с родными в случае, если она/он стали жертвой кибербуллинга.

Расскажите детям, что нужно быть осторожными при общении с незнакомыми людьми онлайн. Интернет-знакомства могут быть опасными — злоумышленники могут выдавать себя за друзей и манипулировать ребёнком в личных корыстных целях.

Эксплуатация и насилие

Сексуализированное насилие и эксплуатация детей могут происходить и онлайн. Например, следующим образом:

Личные фотографии ребёнка могут быть использованы для создания и распространения материалов откровенного характера.

Детей посредством текстового или видео-общения могут принуждать выполнять определённые действия, например, просматривать или делиться изображениями или видео сексуального характера.

Злоумышленники могут использовать интернет для груминга детей, чтобы добиться встреч в реальной жизни.

Груминг — это процесс, при котором взрослый человек устанавливает доверительные отношения с ребёнком для последующего сексуального контакта, как онлайн, так и оффлайн.

Важно говорить с детьми о личных границах, ответственности и важности конфиденциальности в интернете. Необходимо, чтобы ребёнок понимал, что информация в Сети распространяется очень быстро, а полностью удалить её практически невозможно. Поощряйте детей сообщать вам о любых попытках со стороны других людей заставить их делать что-либо, что вызывает дискомфорт. Объясните, что лучше не встречаться с онлайн-знакомыми в реальной жизни без родительского разрешения.

Подводя итоги, сформулируем общие рекомендации.

1. Стройте доверительные отношения с детьми и будьте открытыми.

Открытый диалог с ребёнком о безопасности в интернете — одна из главных мер, которые родители могут предпринять. Важно рассказать детям о том, кому из взрослых они могут довериться, поделиться тем, что беспокоит. Объясните, что вы говорите на эту тему, потому что хотите, чтобы дети были в безопасности. Такой диалог может быть разным в силу возраста ребёнка. Не забывайте о личных границах.

2. Установите чёткие правила поведения в интернете вместе с ребёнком.

Поговорите с детьми о том, с кем и как они общаются онлайн, и кто может видеть их публикации. Расскажите о правилах поведения в интернете (нетикете): недопустимости дискриминационного или неподобающего контента, о важности соблюдения личных границ, умении говорить «нет» неподобающим просьбам как в физическом, так и в виртуальном мире. Объясните, что всё, что размещается в интернете — фотографии, видео, комментарии — оставляет след. Помогите детям научиться распознавать угрозы онлайн и обсудите, как себя вести в каждом конкретном случае.

3. Используйте программы и приложения для защиты.

Обновляйте ПО и приложения на устройстве и настраивайте параметры конфиденциальности. Говоря с детьми о важности хранения личной информации в тайне, не забывайте соблюдать это правило сами. Используйте родительский контроль и инструменты безопасного поиска, например Google Family Link, встроенные экранное время и локатор в iOS. По ссылке можно скачать инструкцию о том, как работает родительский контроль, и какие есть инструменты для разных устройств.

Родительский контроль — это настройки, доступные на всех устройствах и приложениях. Они позволяют родителям управлять экранным временем на устройстве ребёнка, внутриигровыми расходами, контентом, общением онлайн и многим другим.

4. Проводите время в интернете вместе.

Выбирайте подходящие приложения и игры вместе с ребёнком. Для этого можно воспользоваться поисковиком Kids Search или Kidtopia для школьников

младших школ или просто безопасным поиском. Он скрывает контент для взрослых из результатов поиска.

Дети обычно повторяют то, что делают взрослые. Подавайте пример, будьте внимательны к тому, что сами делаете и чем делитесь онлайн. Моделируйте здоровые онлайн-привычки.

5. Этичный родительский контроль

Часто дети лучше разбираются в технологиях, чем их родители. Важно объяснить ребёнку, что родительский контроль устанавливается не для ограничения его прав и контроля, а для его безопасности. Школьнику младшего класса достаточно показать, как работает эта программа. Подростку можно предложить установить приложение самостоятельно и вместе выбрать функции, которые вы будете использовать.

Многие дети знают, как обойти ограничения: создают поддельный аккаунт или используют приложение для взлома. Если ребёнок против установки родительского контроля, не настаивайте. Вернитесь к разговору позже и попытайтесь рассказать о пользе такой программы. Параллельно убедитесь, что ребёнок знает об онлайн-угрозах и способах защитить себя.

Защита детей в интернете требует постоянного внимания и открытого и доверительного общения. Важно, чтобы дети знали, что они могут рассчитывать на вашу поддержку и помощь в любых ситуациях.

Данный материал финансируется Европейским Союзом. Его содержание является исключительной ответственностью команды проекта «Дети&Сети» и не обязательно отражает точку зрения Европейского Союза.

Команда проекта «Дети&Сети»:
Мөлдір Утегенова
Михаил Беляков
Катерина Афанасьева
Насиба Нуритдинова