СБЕРБАНК

СБЕРБАНК ДЛЯ ДЕТЕЙ И РОДИТЕЛЕЙ

ВКЛАД В БУДУЩЕЕ
Благотворительный фонд Сбербанка

SCS SBERBANK CYBER SECURITY

Цифровые джунгли: правила самосохранения

Содержание

Введение

В **предыдущем дайджесте** мы говорили о том, как изменилось представление о грамотности в XXI веке в связи с широким распространением информационных и цифровых технологий. В этот раз мы хотим рассказать, как избегать рисков и опасностей нового цифрового мира, иными словами — о кибербезопасности.

Неумеренное использование детьми гаджетов, круглосуточная ловля покемонов, кибербуллинг, финансовое мошенничество в соцсетях... Чего действительно следует опасаться, а что ребенок «перерастет»?

Цель этого дайджеста — вместе проанализировать основные родительские тревоги, сделать тему безопасности в киберпространстве понятной, а значит – комфортной, и дать практические инструменты, которые помогут сделать использование цифровых технологий в повседневной жизни безопасным для вас и ваших детей.

Кибербезопасность: с чего начать

Необходимость в базовых знаниях о кибербезопасности возникает в момент, когда ребенок в первый раз берет в руки планшет или смартфон. Цифровые технологии и связанные с ними риски постоянно эволюционируют, и вместе с ними меняются технические способы защиты. Но не от всех угроз возможно защититься технически: большинство схем мошенничества в Сети строится еще и на психологических манипуляциях. Поэтому важно понимать, что оградить себя и детей от рисков в цифровом мире помогает умение эффективно пользоваться средствами защиты и противостоять психологическим уловкам.

Чтобы более ясно понимать, с какими интернет-рисками чаще всего сталкиваются подростки, и как уровень осведомленности в области кибербезопасности взрослых помогает их снизить, рекомендуем познакомиться с результатами исследования **Фонда развития Интернета при факультете психологии МГУ имени М. В. Ломоносова**.

С чего же начать родителям?

Во-первых, научиться хорошо разбираться в вопросах кибербезопасности самим. Знать термины, понимать, где подстерегают угрозы, какие способы профилактики можно использовать самостоятельно, а в каких случаях необходимо советоваться со специалистами.

Во-вторых, учить личным примером и чаще пользоваться смартфоном или планшетом вместе с ребенком и комментировать свое поведение — так основные правила безопасности будут усвоены лучше.

В-третьих, разговаривать с ребенком о возможных рисках и вместе исследовать, как лучше всего их избегать. Старайтесь объяснить заранее: дошкольнику — почему нельзя «кликать», если что-то вдруг ярко замигало на экране; подростку — о правиле Log out, и почему не стоит публиковать личные фотографии «ВКонтакте»; и всем — о том, что «доверяй, но проверяй» не просто пословица, а главное правило грамотного пользователя цифровых технологий.

И самое главное — старайтесь выстраивать доверительные отношения. Важно, чтобы ребенок понимал, что в любой непонятной или пугающей ситуации вы — его лучший союзник и будете вместе с ним искать безопасное решение.

Начать уверенное освоение безопасного киберпространства вам поможет **словарик основных понятий, подготовленный Денисом Гамаюновым** — заведующим лабораторией безопасности информационных систем факультета вычислительной математики и кибернетики МГУ им. М. В. Ломоносова.

А чтобы проверить, насколько хорошо вы знакомы с киберугрозами (как настоящими, так и фейковыми), попробуйте пройти **занимательный тест** от «ПостНауки» сами или предложите подростку пройти его вместе. Скучно не будет!

Как безопасно пользоваться компьютером и гаджетами

Проще всего организацию кибербезопасности начать с антивирусной защиты ноутбуков, смартфонов и планшетов. Даже если вы осторожный пользователь — не открываете подозрительные письма и не посещаете сомнительные сайты, — увернуться от вирусной атаки удается не всегда. Злоумышленники научились не только «подсаживать» вирусы на компьютеры, но и взламывать мобильные устройства.

Начните с установки качественной антивирусной программы на все устройства, которыми пользуются в вашей семье, и не забывайте ее регулярно обновлять (для операционных систем, отличных от iOS). Следуйте памяткам, подготовленным Лабораторией Касперского — они помогут защитить устройства от основных угроз. Для операционной системы iOS (iPhone, iPad, Mac) не забывайте устанавливать обновления программного обеспечения.

Как защитить компьютер и ноутбук

- Убедитесь, что на всех устройствах установлена антивирусная программа/обновлено программное обеспечение и следуйте рекомендациям. Они защитят от самых распространенных интернет-атак.

- Не экономьте, качая файлы со сторонних (возможно, зараженных) ресурсов, лучше загрузите их с сайта разработчика.

- Не запускайте программы, присланные незнакомцами. Все проверяйте антивирусной программой. Даже самый маленький файл может содержать большой вирус, который способен украсть пароли и удалить файлы с компьютера.

- Даже если письмо с программой прислал друг или член семьи — проверьте, не взломан ли его аккаунт. Мошенники часто рассылают вирусы от имени других людей. Письмо с подозрительной ссылкой может стать причиной заражения вашего компьютера.

Как распознать мошенническое письмо

Как защитить смартфон

- Установите пароль на свой мобильный, чтобы посторонние не могли заходить в приложения и видеть личную информацию.

- Убедитесь, что на устройстве установлена антивирусная программа/обновлено программное обеспечение.

- Старайтесь не использовать открытые Wi-Fi-точки для передачи личной информации и проведения платежных операций.

- Активируйте опции удаленного управления с помощью настроек телефона или специального приложения — так вы сможете контролировать устройство удаленно, даже если его украли.

- Вирусы поражают и смартфоны тоже. Не качайте незнакомые приложения даже из официальных магазинов. Всегда проверяйте список запрашиваемых приложением разрешений, таких как покупки из приложений, доступ к списку контактов и так далее.

- Не переходите по ссылкам в подозрительных смс-сообщениях. **Пройдите тест сами или вместе с подростком** и проверьте, сможете ли вы понять, что смс или личное сообщение написал мошенник.

О том, что такое компьютерный вирус, чем он опасен и как его «вылечить», самым маленьким пользователям **расскажут герои мультсериала «Фиксики»**

Как оградить ребенка от нежелательного контента

Интернет — это пространство, созданное взрослыми для взрослых. Если в кинотеатрах и на телевидении у каждой программы есть возрастной рейтинг, то в мировой Сети канал с детскими мультфильмами от сайта с взрослым, пугающим или опасным для детской психики содержанием может отделять всего один клик. Оградить ребенка от нежелательного контента — одна из главных задач для взрослых.

Пока дети маленькие, на помощь придут средства родительского контроля и настройки безопасности интернет-браузеров. Антивирусные программы и последние версии операционных систем уже содержат функции родительского контроля, а самые популярные браузеры предлагают варианты блокировки сайтов и фильтры безопасного поиска информации.

Что такое программы родительского контроля и какие технические средства можно использовать, чтобы оградить ребенка от нежелательного контента, **читайте в обзоре портала «Семейный эксперт».**

Научитесь настраивать безопасный семейный поиск:

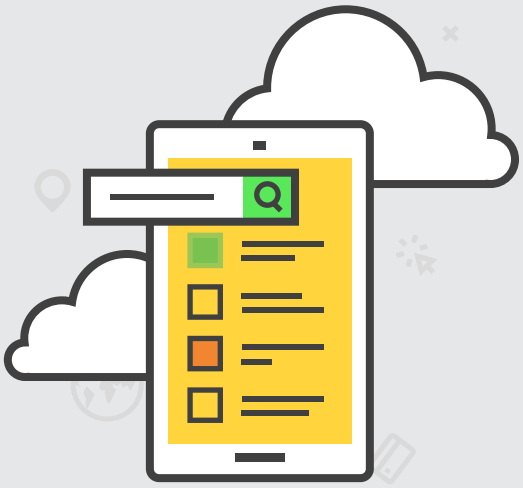
в браузере Google Chrome

в «Яндексе».

Познакомьтесь с возможностями 10 бесплатных программ для безопасности ребенка по версии интернет-издания RUSBASE.

Но это техническая сторона вопроса. Фильтры на домашних устройствах не оградят ребенка от информации, которой делятся с ним одноклассники или друзья, а подросток сможет легко поменять настройки браузера или операционной системы. Поэтому гораздо важнее стараться обсуждать с детьми, в чем опасность тех или иных видов информации; помогать развивать критическое мышление и устойчивость психики к возможному давлению.

Оптимальный вариант — предлагать вместе исследовать игры, сайты и видео в Сети. Старайтесь разговаривать о том, что не весь контент рассчитан на детей и подростков, что он может быть пугающим и просто опасным. Важно, чтобы ребенок знал: он всегда может смело поговорить с вами о любых проблемах или некомфортном общении в Сети.



Как защитить персональные данные в публичном пространстве

Персональные данные или личная информация — номер социального страхования и паспорта, номер телефона ваш или родственников, ИНН, домашний адрес, дата рождения, подтверждающие пароли, ПИН- и CVV-коды от банковских карт — одни из самых лакомых кусочков для интернет-мошенников. Именно эти сведения являются целью вирусных и психологических атак злоумышленников.

К личной информации относятся фотографии дорогих вещей, документов (дипломов, виз, паспортов), а также статусы о том, что вы всей семьей отправляетесь в путешествие. Сделанные с помощью смартфона снимки имеют геотеги, а селфи на фоне дома, школы или офиса прямо указывают, где можно найти вас, вашего ребенка или ценные вещи у вас дома.

Чтобы защитить персональные данные, для начала поговорите со своей семьей о том, какие сведения о себе нельзя размещать в интернете, а какие — можно только на сайтах, которым вы доверяете. Следуйте правилу: если сомневаюсь, можно ли доверить информацию о себе этому сайту, то делать этого не буду. Договоритесь, о каких событиях в личной жизни и жизни семьи не стоит писать в интернете, и объясните почему. Расскажите ребенку, что даже если он размещает информацию о себе только для друзей, особенно деликатную, ее могут использовать против него интернет-тролли — после ссоры с другом или если аккаунт кого-то из друзей будет взломан.

YouTube — одна из самых популярных сетей среди детей и подростков. Научитесь устанавливать **безопасный режим** на всех устройствах (его нужно устанавливать в каждом браузере отдельно) и не забывайте о **настройках конфиденциальности**.

Защитить вашу конфиденциальность в Сети поможет знакомство с файлами cookie. Это временные файлы, которые сохраняются в браузере и помогают сайту запоминать информацию о вас: логин и пароль, на каком языке вы просматриваете информацию, предпочтения и т.д. На первый взгляд они не опасны, но в некоторых случаях могут принести вред пользователям. **Подробнее о том, что нужно знать о файлах cookie, рассказывают эксперты Лаборатории Касперского.**

Настроить прием файлов cookie, удалить или настроить автоочистку помогут **инструкции для различных браузеров** от «Яндекс», а **гид по защите личной информации** поможет обобщить рекомендации этого раздела.

Как безопасно распоряжаться финансами в цифровом мире

Конечной целью кражи личных данных в интернете почти всегда выступает ваш кошелек, а большинство усилий мошенников направлено на получение платежной информации: номеров кредитных карт, паролей к интернет-банкингу, CVV-кодов.

Банки и современные платежные системы постоянно совершенствуют системы безопасности, чтобы защитить деньги и персональные данные своих клиентов. Но технические средства не смогут защитить, если вы лично не будете соблюдать осторожность. В этом разделе мы собрали материалы, которые помогут взрослым и подросткам научиться безопасно распоряжаться финансами при использовании цифровых технологий.

Банковские карты и онлайн-платежи

Начните с соблюдения базовых правил безопасности при использовании цифровых устройств:

- Не сообщайте никому, даже сотрудникам банка, свои подтверждающие пароли, ПИН- и CVV-коды от банковских карт.
- Используйте только официальные банковские приложения Сбербанка из магазинов App Store, Google Play, Windows Store.
- Если вы сменили номер мобильного телефона, позвоните в банк и сообщите об этом, чтобы ваши данные не попали новому владельцу номера.
- Используйте антивирус. Установите на телефон Android-приложение «Сбербанк Онлайн» с бесплатным антивирусом.
- Не переходите по сомнительным ссылкам на незнакомые ресурсы: мошенники могут заразить ваш компьютер или телефон вирусом и украсть ваши личные данные.
- Проверяйте реквизиты операции в СМС от банка с подтверждающим паролем.

И устройств самообслуживания:

- Прикрывайте клавиатуру рукой, когда вводите ПИН-код.
- Подключайте СМС-сервис «Мобильный банк» только на свой номер телефона. Переводите деньги только известным вам получателям.
- Вход в зоны самообслуживания не требует ввода ПИН-кода вашей карты.

Запомнить важнейшие правила безопасного использования онлайн-сервисов Сбербанка поможет наглядный ролик.

Подробные инструкции о том, как безопасно пользоваться мобильным приложением и интернет-банком Сбербанка, как обезопасить себя от e-mail- и телефонного мошенничества и что делать, если вы пострадали от мошенников, вы найдете в разделе «Ваша безопасность» на сайте Сбербанка.

А что же контактные и бесконтактные платежные средства? Могут ли мошенники списывать с них суммы или использовать данные без нашего ведома? Нет, если соблюдать базовые правила безопасности:

→ как безопасно расплачиваться банковской картой

→ что нужно знать об использовании бесконтактных карт

Финансовое мошенничество в соцсетях

Увы, стать жертвой мошенников можно не только в интернет-магазине или снимая деньги в банкомате. Все чаще злоумышленники используют в своих целях соцсети. Они могут представляться сотрудником банка или предлагать поучаствовать в опросе банка за вознаграждение и призы.

Понять, что вы имеете дело с мошенниками, поможет простая инструкция на канале Сбербанка сервиса «Яндекс.Дзен»

Интернет-лотереи и выигрыши

Не будем забывать об интернет-лотереях и других внезапных «выигрышах» в конкурсах, в которых вы не участвовали. Если вдруг вы оказались миллионным посетителем незнакомого сайта или получили письмо о выигрыше в лотерее, не спешите радоваться, скорее всего это не что иное, как один из видов фишинга с целью получить ваши персональные данные или деньги.

Чтобы не стать жертвой мошенничества, помните о простых правилах:

1. Невозможно выиграть приз в лотерее, в которой вы не участвовали. Акции, в которых приз получает миллионный посетитель сайта, иногда действительно проводят крупные компании — в этом случае информация о таком розыгрыше публикуется заранее и ее можно проверить по официальным источникам.

2. Любые просьбы «организаторов лотереи» о внесении налога или иной суммы денег ДО получения приза — признак мошенничества. Все налоги и сборы выигравший платит сам ПОСЛЕ получения приза.

3. Если хочется поверить в выигрыш, тщательно проверьте всю информацию о розыгрыше в интернете: сведения о компании-организаторе, официальные правила розыгрыша, имена и телефоны отправителей сообщения. Иногда мошенники создают целые сайты с именами «победителей» — проверяйте адрес сайта и реквизиты компании-организатора.

4. Письма с ошибками или явно переведенные через автоматический переводчик — еще один признак мошенничества. Проверьте e-mail, с которого пришло уведомление: организаторы лотерей не используют бесплатные почтовые сервисы.

5. И никогда не забывайте: бесплатный сыр бывает только в мышеловке.

6. Подросткам: письма счастья, заманчивые конкурсы и веселые тесты могут обернуться **зараженным компьютером или украденной личной информацией**.

Приложения со встроенными покупками и подписки

Игры и приложения со встроенными покупками тоже могут влиять на ваше финансовое положение. Многие бесплатные приложения предлагают совершать покупки в процессе игры: чтобы открыть новый уровень, увеличить скорость персонажа, получить редкие артефакты. Детские игры — лидеры среди таких приложений.

Дети могут даже не подозревать, что игровая валюта — это реальные денежные средства, да и сами взрослые в азарте игры нередко забывают о том, что конвертируют виртуальные деньги в реальные. Разработчики вкладывают силы и средства в создание игры или приложения, поэтому желание получить вознаграждение понятно и оправдано. Проблема в неконтролируемой трате средств: покупки во время игры кажутся особенно соблазнительными, а связь с реальными деньгами — не очевидной.

Лучшее средство защиты от чрезмерных игровых трат — по возможности не привязывать банковскую карту к устройству, на котором играете вы или ребенок. Если же карта привязана, не забудьте настроить **функцию ограничения покупок:**

→ как это сделать на устройствах Apple

→ как это сделать на Google Android

Но не стоит полагаться только на технические средства. Объясните ребенку, что внутриигровые покупки тратят реальные деньги, а сумма должна быть соразмерна удовольствию от игры и возможностям семейного бюджета. Постарайтесь договориться, что если ребенок захочет что-то купить во время игры, он сначала обратится к вам.

Подробнее о правилах, которые помогут избежать чрезмерных внутриигровых покупок на планшетах и игровых консолях, а также о том, какие финансовые ловушки скрывают браузерные, традиционные и сетевых игры, читайте в статье **«Как ограничить покупки в играх»**, подготовленной Лабораторией Касперского.

Платные (и бесплатные, но переходящие в платные) подписки на смартфонах тоже могут стать для вас причиной головной боли и незапланированных финансовых трат. Изучите инструкции и научитесь вовремя **отключать или изменять платную подписку**, если она вам больше не нужна:

→ на устройствах Apple

→ на устройствах Google Android

Финансы и безопасность в цифровом мире для подростков

Старайтесь заранее рассказать ребенку об основных финансовых рисках и уловках мошенников, которые подстерегают в интернете. Если же подросток уже распоряжается карманными деньгами самостоятельно, ресурсы ниже помогут систематизировать и закрепить эти знания.

Курс «Безопасность в интернете» портала «Yandex.Деньги» рассчитан на школьников 6—9-х классов, но будет полезен и интересен даже взрослым. Вирусы, кража паролей и многое другое — **курс поможет не оказаться жертвой манипуляций мошенников**.

Красочные и подробные советы подросткам по безопасности дает программа «Финансовая грамотность» Благотворительного фонда Сбербанка «Вклад в будущее», разработанная совместно с издательством «Манн, Иванов, Фербер»: воображаемый друг, счастливый обладатель приза, сетевые ловушки и другие уловки мошенников, о которых обязательно нужно знать. (**Использованы материалы из блокнота-челленджа «Твои финансы. Планируй, копи и трать с умом»**)

Как избежать опасностей в соцсетях

Как бы нам ни хотелось, чтобы дети больше времени проводили на улице, общались и играли офлайн, новые форматы коммуникации диктуют свои условия. Живого общения становится все меньше, зато круглые сутки ребенок на связи в социальных сетях. Начиная с 11—14 лет подросток заводит собственный аккаунт «*ВКонтакте*», на *Facebook* или *Tumblr*, и с этого момента он «дрейфует» в сети. Окажется ли этот дрейф безопасным, во многом зависит от родителей.

Социальные сети — это не только друзья и общение по интересам, это еще и место обитания троллей, агрессоров, вербовщиков, мошенников и даже извращенцев. Как же защититься?

Важнее попыток контролировать, с кем ребенок общается, рассказать ему о возможных рисках. И взрослых, и детей в интернете подстерегают две главные ошибки: ощущение, что общение онлайн — только игра, понарошку, и непонимание того, насколько много знакомых и незнакомых людей увидят каждое слово, сказанное в Сети.

Никогда не пиши в интернете того, что не сможешь сказать человеку в лицо, стоя перед всем классом и всеми знакомыми

Это самое важное правило, которое подросток должен усвоить перед тем, как начать пользоваться соцсетями и общаться в интернете.

Зная, чем ребенок интересуется, на каких сайтах бывает, чем делится, можно предусмотреть возможные угрозы и предупредить о них подростка. **Простые правила безопасности в соцсетях от Лаборатории Касперского** помогут сделать это наиболее эффективно.

Тема суицида страшна сама по себе, а когда она касается подростков, то первая реакция родителей — запрет, табу. Именно поэтому история об игре «Синий кит» и **«группах смерти»** в социальной сети «ВКонтакте» вызвала такую волну паники. Основной совет психологов в подобной ситуации: не увеличивать число запретов и не избегать разговоров на «опасные темы» с подростком.

Разработанную психологами инструкцию о том, как избавиться от тревоги и что нужно делать, если ребенок заинтересовался «группами смерти», можно изучить на портале Meduza.

Что делать родителям, когда вокруг разрастается паника из-за «групп смерти», и о чем действительно стоит беспокоиться, **рассказывает практикующий семейный психолог Катерина Дёмина**.

Кибербуллинг — другая большая проблема, которая появилась одновременно с онлайн-общением. Школьная и дворовая травля незаметно перебралась и закрепилась в Сети. Последние исследования Microsoft и Всемирной организации здравоохранения показывают, что не меньше 65% взрослых и подростков хотя бы раз сталкивались с кибербуллингом. При этом из 42 стран, участвовавших в опросах, Россия занимает первое место по кибербуллингу среди детей до 11 лет: как девочки, так и мальчики получают сообщения с оскорблениями не менее двух-трех раз в месяц. Подростки старше с травлей сталкиваются реже.

О том, что такое кибербуллинг и как противостоять троллям, наглядно и просто объясняется **в ролике, созданном каналом «Научпок» в сотрудничестве с ИИТО ЮНЕСКО**.

Если вы подозреваете, что ребенок столкнулся с кибербуллингом, предложите ему ответить на следующие вопросы. Если большинство ответов будут положительными, необходимо принимать меры:

→ Ты получаешь электронные письма или сообщения в социальных сетях с оскорблениями или угрозами, которые предназначены лично тебе?

→ Тебя оскорбляют во время онлайн-игр в сети?

→ На тебя «жалуются» лишь для того, чтобы тебя забанили на сайте или в игре?

→ Тебя преследуют на твоих страницах в социальных сетях, блогах, любимых сайтах (пишут гадости, жалуются)?

→ От твоего имени пишут другим людям ругательства, создают сайты и наполняют ее постыдной информацией, используют твои данные для регистрации на запрещенных или сомнительных сайтах?

Если ваш ребенок стал жертвой травли в Сети, не нужно паниковать. **Воспользуйтесь рекомендациями и советами**, подготовленными экспертами Лаборатории Касперского, которые помогут разрешить проблему.

В борьбе с кибербуллингом помогает не только психологическая защита, но и современные технологии. **Обзор специальных программ по борьбе с кибербуллингом**, разработанных совместно с Институтом ЮНЕСКО по информационным технологиям в образовании, поможет в них разобраться.

Как и в случае с другими видами киберугроз, лучший способ снизить риски — поговорить с подростком о проблеме и дать инструменты, которые помогут ее предотвратить. **Десять простых советов по защите от кибербуллинга помогут подростку защитить себя от травли и ее последствий**.

Как бороться с зависимостью от гаджетов

Мы много говорили об угрозах, которые поджидают детей в Сети и при онлайн-общении. Но существует и еще одна важная психологическая проблема — зависимость от гаджетов. Врачи предупреждают, что чрезмерное пребывание ребенка перед монитором компьютера, экраном планшета или смартфона может приводить к ожирению, отставанию в развитии, проблемам со сном и депрессиям.

Чтобы понять, пора ли бить тревогу из-за привязанности ребенка к гаджетам или оснований для беспокойства все же нет, попробуйте провести небольшой **тест, опубликованный на портале «Безопасность в интернете»**.

Предложите ребенку по возможности честно ответить «да» или «нет» на следующие утверждения (если сложно отвечать устно, ответы можно написать на листочке бумаги):

- Не могу даже дня провести без компьютера, смартфона или других гаджетов.
- Когда под рукой нет гаджета, я начинаю нервничать.

➔ Не контролирую время использования смартфона или компьютера — всегда сижу дольше, чем планировал.

➔ Не говорю родителям, сколько времени на самом деле провожу за игрой или в соцсетях.

➔ Все, о чем мечтаю — наконец остаться один на один со смартфоном.

➔ Если в руках планшет, не могу сосредоточиться на уроках — всё время отвлекаюсь на что-нибудь в Сети.

➔ Когда я сижу за компьютером или с планшетом, у меня всегда хорошее настроение, эйфория.

➔ Постоянно требую от родителей новых версий игры, покупки дополнительных свойств, новых гаджетов.

➔ Иногда после длительного пользования устройствами у меня болит голова, возникают рези в глазах, появляется бессонница (достаточно одного признака для положительного ответа).

➔ Предпочитаю играть на компьютере, чем гулять и встречаться с друзьями.

Посчитайте ответы «Да»:
1—4 — поводов для беспокойства нет;
5—6 — существует тенденция к зависимости;
7—10 — наблюдается зависимость от гаджетов.

Как поступить, если повод для беспокойства все же есть? Советы специалистов можно свести к трем основным группам:

1. Соблюдать всей семьей цифровую гигиену: договариваться об ограничениях в использовании гаджетов и стараться соблюдать их всем вместе, подавать личный пример.
2. Находить вместе или предлагать увлекательные альтернативы: походы, спорт, экскурсии, настольные игры и умные конструкторы.
3. Стараться освобождать время для живого общения с ребенком — только оно может конкурировать по привлекательности с компьютерными играми и социальными сетями. Ведь чтобы помочь ребенку избавиться от цифровой зависимости, от вас обоих потребуется одинаковое количество внимания.

Разобраться в проблеме помогут советы, подготовленные порталом Meduza с участием семейного психотерапевта Инны Хамитовой, руководителя проекта «Раннее инженерное развитие детей» Анатолия Шперха и старшего научного сотрудника лаборатории когнитивных исследований РАНХИГС Кирилла Хломова.

Заключение

В этом дайджесте мы познакомились с основными аспектами кибербезопасности: научились разбираться в базовых терминах, рассмотрели самые распространенные риски, освоили инструменты, которые помогают их предотвращать.

Увидели, что **важно не пугаться рисков в интернете**, а «знать их в лицо», уметь находить **инструкции по безопасности** для каждой ситуации и следовать ей вместе с ребенком. Узнали, как оградить детей от нежелательного контента, защитить персональные данные и деньги от злоумышленников, как безопасно общаться в соцсетях, противостоять кибербуллингу и преодолевать зависимость от гаджетов.

Надеемся, что **советы специалистов и собранные материалы** помогут вам и вашим детям **чувствовать себя более уверенно и спокойно** при использовании цифровых технологий в повседневной жизни: общаться и заводить друзей, учиться и осваивать новые навыки, работать, совершать покупки, пользоваться онлайн-сервисами.

Быть грамотным в XXI веке в числе прочего означает уметь максимально безопасно реализовывать возможности, которые предоставляет информационная и цифровая среда для эффективного развития, жизни и учебы в современном обществе. Используйте для этого инструменты, представленные в дайджесте, и научите пользоваться ими своих детей.

Материалы подготовлены при экспертной и методической поддержке специалистов Благотворительного фонда Сбербанка «Вклад в будущее».

Фонд реализует программу «Учить учиться», нацеленную на выявление, разработку и распространение лучших практик развития у детей желания и умения учиться.

Над выпуском также работала редакция компании Smart Course.

Полезные ресурсы

Сайт «Защита детей» Лаборатории Касперского

Центр безопасности Google

Советы для родителей Центра безопасности Facebook

Федеральная программа безопасного детского интернета «Гогуль»

Лекция Галины Солдатовой «Цифровое поколение: компетентность и безопасность». Часть 1-я и часть 2-я

Лекция Станислава Кузнецова (Сбербанк) «Кибербезопасность — как защититься в мире киберугроз?»

Лекция для подростков Антона Карпова («Яндекс») «Информационная безопасность — мир «белых и черных шляп»