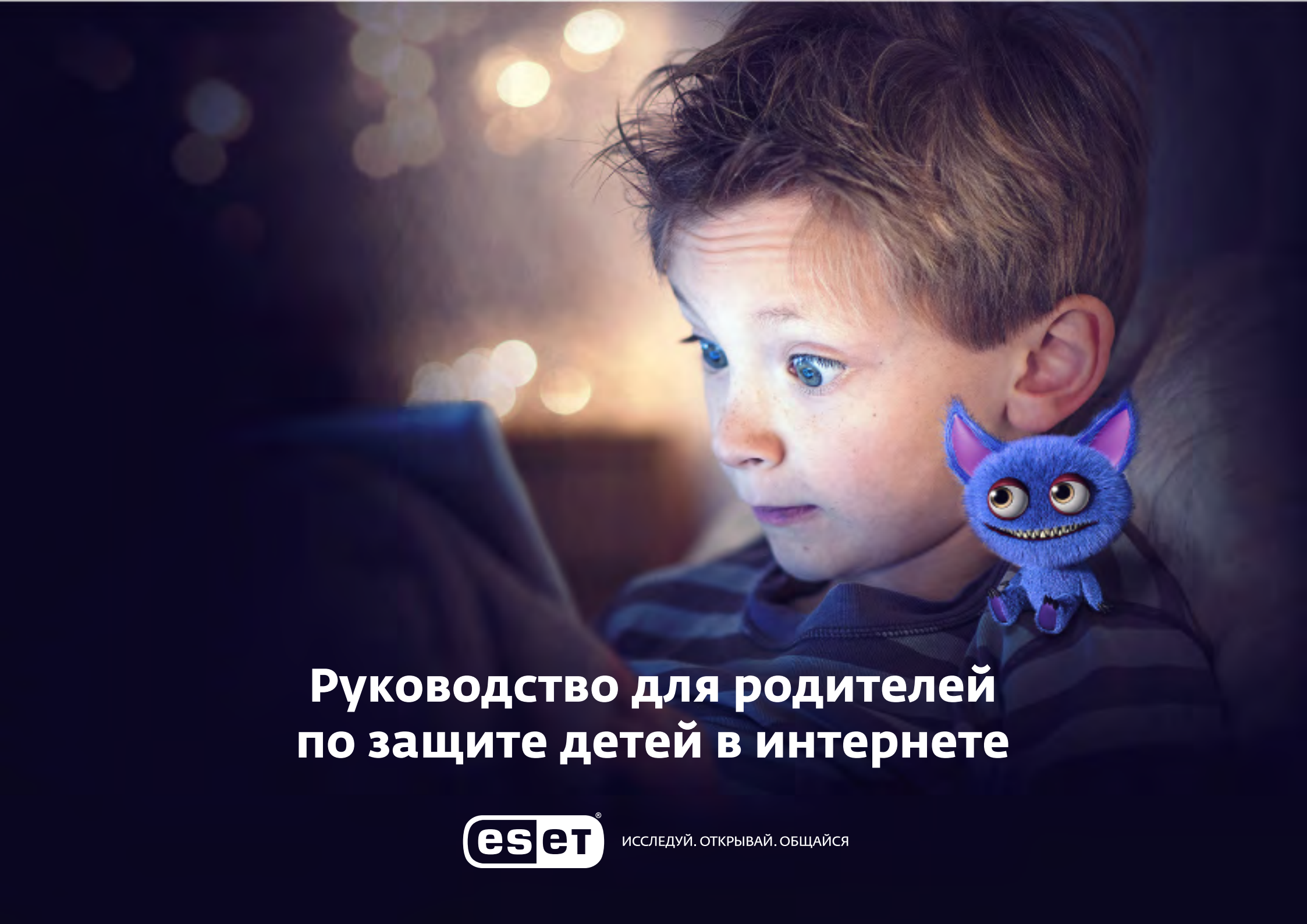


Руководство для родителей по защите детей в интернете

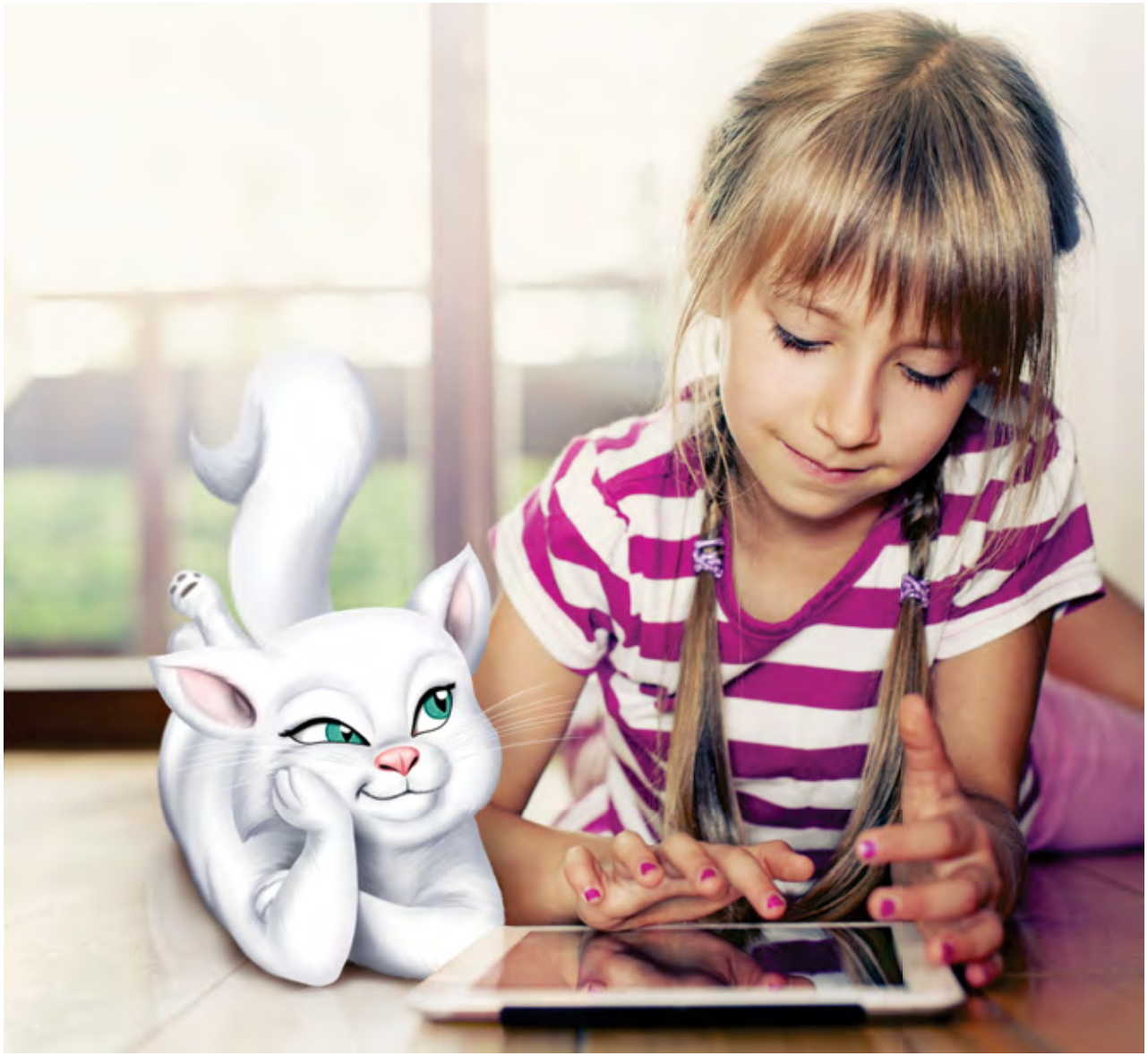
ИССЛЕДУЙ. ОТКРЫВАЙ. ОБЩАЙСЯ

Предисловие

Наши дети – главная ценность в жизни, наше будущее. У сотрудников ESET тоже есть дети, о безопасности которых необходимо позаботиться. Однако в наше время защищать ребенка от различных неприятностей – непростая задача.

Современные телефоны и планшеты становятся все сложнее. В связи с этим родителям необходимо постоянно совершенствовать свои знания технологий, чтобы помогать детям правильно использовать гаджеты.

Данное руководство призвано помочь родителям защитить маленьких пользователей мобильных устройств и интернета.



Кто должен начать разговор?

Мы понимаем, что безопасность в интернете – достаточно сложная тема. Поэтому, именно вы должны инициировать этот разговор с ребенком.

На протяжении всей своей жизни ваши дети будут встречать важных для себя людей: родственников, друзей, учителей.

Тем не менее, ни один из них не сможет заменить вас как родителя. В глазах ребенка вы являетесь источником правильных ответов на все вопросы и помощником в сложные моменты, когда он не знает, что делать дальше.

Когда начать этот разговор?

Как можно скорее. Лучше прямо сейчас.

Чем старше становятся дети, тем больше новых проблем появляется. В незнакомой ситуации полезный совет от близкого человека может стать решающим моментом, который подтолкнет ребенка в правильном направлении в будущем. Такой совет важен, в том числе и когда речь идет о киберпространстве.

Как только ребенок начинает проявлять интерес к вашему планшету, смартфону или компьютеру с доступом в интернет, пора объяснить, что все, что он знает о безопасности в реальной жизни, относится и к интернету. Среда меняется, но угрозы остаются прежними.

Родители учат своих детей и учатся сами

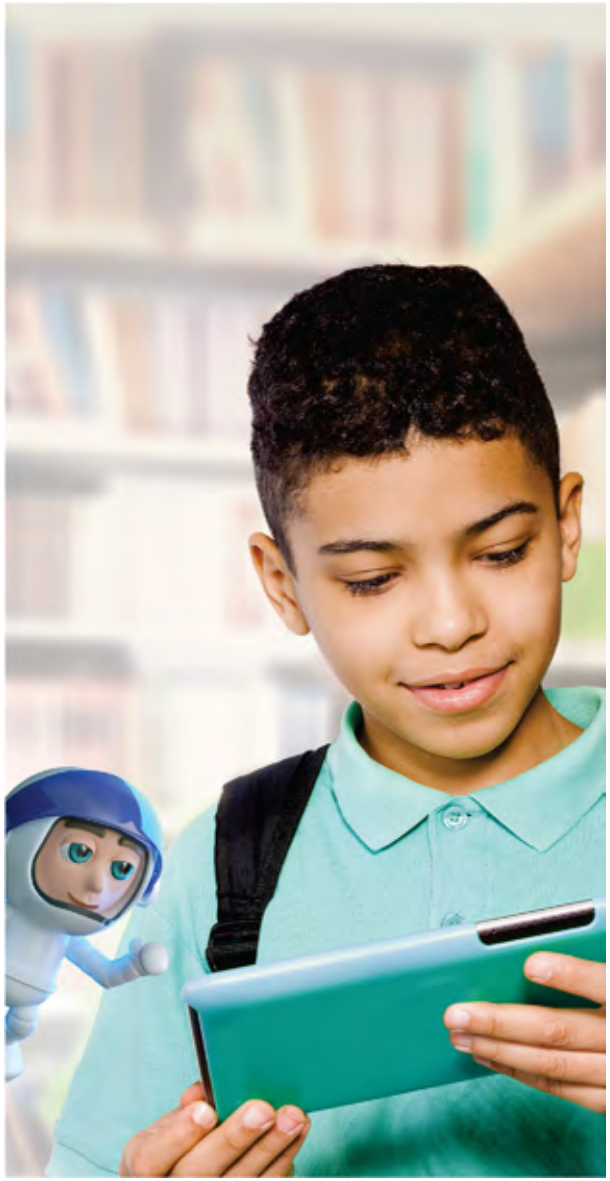
Вам кажется, что дети знают о компьютерных технологиях больше, чем вы? Вы не одиноки, многие родители думают точно так же.

Нынешние подростки родились буквально со смартфоном в руках, в то время как взрослые познакомились с мобильными устройствами уже в сознательном возрасте.

Но это не делает ребенка главным техническим специалистом в доме. Даже если дети умеют пользоваться интернетом, это не означает, что они осознают последствия каждого действия в Сети.

Родителям нет необходимости разбираться в цифровом мире лучше детей.

Но вы должны быть всегда готовы к моменту, когда ваш ребенок найдет в Сети что-то незнакомое и будет нуждаться в разговоре с взрослым человеком.
Необходимо вовлечь ребенка в диалог. Поэтому в семье так важна доверительная атмосфера, где дети могут свободно задавать вопросы и получать исчерпывающую информацию в доступной форме.



Сколько лет вашему ребенку?

Далее мы расскажем об инструментах
и способах обеспечения безопасности детей
в интернете в соответствии с их возрастом.

МЛАДШЕ 10 ЛЕТ

1. Делайте первые шаги в интернете вместе

Будьте рядом, когда ваши дети делают первые шаги в Сети. Лучший формат первого знакомства ребенка с интернетом – отправиться в это путешествие вместе с родителями.

2. Разработайте правила

Установите базовые правила для использования интернета. Вы можете контролировать количество часов, проведенных в Сети, и задать временные интервалы, в течение которых можно пользоваться интернетом.

3. Покажите пример

Дети зачастую копируют поведение своих родителей. Это правило работает как для реального мира, так и для цифрового – ребенок перенимает правильные привычки в интернете.

ОТ 10 ДО 13 ЛЕТ

1. Используйте программы для родительского контроля

Используйте современные технологии. Так, мобильное приложение ESET NOD32 Parental Control для Android позволяет блокировать неприемлемые веб-страницы и категории сайтов с нежелательным контентом. Вы можете устанавливать временные ограничения на использование интернета и игр. При этом ребенок всегда может попросить у вас разрешение посетить определенный сайт или выделить больше времени на игры, если он уже сделал уроки.

2. Расскажите детям, как опасно делиться личной информацией

Очень важно донести до ребенка мысль, что в виртуальном мире не каждый человек является другом. Объясните, почему так опасно делиться личной информацией, включая домашний адрес, номер телефона, расписание школьных и внешкольных занятий и др. Договоритесь с ребенком, чтобы он спрашивал у вас разрешение перед загрузкой личных фотографий в Сети.

3. Будьте открыты к диалогу

Попросите ваших детей быть открытыми с вами и свободно обсуждайте с ними то, что они видят в интернете. Если это возможно, поставьте компьютер в общей комнате, где проводит время семья, чтобы ребенок был в поле зрения.

ОТ 14 ДО 18 ЛЕТ

1. Никто не должен знать их пароли

Мы понимаем, что с подростками нелегко, но вы должны убедиться, что они знают основы создания надежных паролей для личных учетных записей. В конце концов, пароль – это то же самое, что ключи от дома. Уважайте личное пространство детей, но будьте уверены, что они никогда не передадут пароли незнакомым людям ни лично, ни через интернет.

2. Попросите их сообщать о случаях издевательства над ними

Помните задир из вашей школы, которые делали жизнь «ботаников» невыносимой? Сегодня таких персонажей можно встретить как в реальном, так и в виртуальном мире, и они продолжают психологически подавлять оппонентов. Поэтому просите своих детей незамедлительно рассказывать вам об издевательстве в Сети.

3. Онлайн-покупки и переводы – только для взрослых

Онлайн-шопинг не влечет негативных последствий, если операция проведена корректно. До тех пор, пока дети не поймут важность защиты онлайн-платежей, они могут делать покупки только под наблюдением родителей.

Словарь кибербезопасности

Дома или в школе

Современные родители несут ответственность за безопасность ребенка как в реальном мире, так и в виртуальности. Однако это не означает, что весь груз ответственности ложится на ваши плечи. Проверьте наличие уроков по информатике и интернет-безопасности в школьном расписании ребенка. Отлично, если эти уроки будет вести учитель, который пользуется авторитетом у учеников – он сможет стать правильной ролевой моделью для подростка, отказывающегося слушаться родителей. Вы дали ребенку базовые знания о безопасности в интернете, школа поможет поднять их на новый уровень.

Родительский контроль

Представьте, что у вас есть специальная программа, которая позволяет устанавливать временные ограничения на использование интернета и игр, показывать ребенку только приемлемые для его возраста сайты и отслеживать текущее местоположение.

Подобные программы называются «Родительский контроль» и являются мощным инструментом для защиты детей в интернете. С другой стороны, такие программы должны давать право голоса и самому ребенку. Иначе, если правила покажутся ребенку слишком суровыми, он найдет способ их обойти.

Социальные сети

Вспомните ваших одноклассников, друзей и просто знакомых. А теперь поместите их в одну комнату, и пусть они обсуждают свои дела, показывают фотографии из отпусков или любимые видеоролики. Именно так работают социальные сети, позволяющие пользователю организовывать мероприятия, общаться с другими людьми тет-а-тет или в группах и видеть, что нравится другим.
Ваш небольшой мир является мизерной частью суперструктуры, включающей сотни миллионов пользователей по всему миру, которые могут общаться в том числе и с вами. С этим связаны как преимущества, так и риски социальных сетей.

Каковы основные угрозы?

Вредоносные программы

Большая часть вредоносных программ создается злоумышленниками для получения финансовой выгоды. Некоторые из них шифруют файлы на вашем компьютере и требуют выкуп за восстановление доступа к данным, другие шпионят за вами или загружают другие опасные программы с удаленного сервера. Например, в 2009 году через Facebook распространялся червь Koobface. Программа отправляла пользователям заманчивые сообщения. Зараженные компьютеры становились частью ботнет-сети – «армии зомби», которой удаленно управлял злоумышленник. Спустя два года появилась новая, более продвинутая модификация Koobface, которая заражала компьютеры пользователей социальной сети независимо от операционной системы: Windows, Mac OS и Linux.
В большинстве случаев заражение происходит из-за ошибки пользователя (или его детей), обманутого злоумышленником.
Применение современных антивирусных продуктов и новейших технологий кибербезопасности снижает риск заражения.

Фишинг

Многие злоумышленники используют для кражи конфиденциальных данных фишинг. Как правило, они присылают по электронной почте ссылку на поддельный сайт, копирующий хорошо знакомую вам площадку (например, интернет-банк или соцсеть). Определить подделку довольно сложно. Дети могут принять поддельный сайт за настоящий и «подарить» злоумышленникам логин и пароль от аккаунта в соцсети.

Кибербуллинг

Кибербуллинг – травля в интернете – это враждебное поведение, довольно часто нацеленное на детей. Как правило, жертву запугивают в киберпространстве сверстники, это явление довольно распространено среди подростков. Такие действия могут нанести вред ребенку и спровоцировать эмоциональную травму. Кибербуллинг обычно происходит в интернете, но ребенок не застрахован от этой проблемы, даже если пользуется только телефоном и игровой приставкой.

Нежелательные ухаживания

Нежелательным ухаживанием можно назвать попытки взрослого человека создать атмосферу доверия с ребенком, чтобы убедить его выполнить определенные сексуальные действия. Взрослые, притворяющиеся друзьями детей, нередко пытаются договориться о личной встрече. Поэтому для родителей очень важно хорошо знать тех, с кем общается их ребенок в интернете.

Секстинг или интимная переписка

Термин «секстинг» происходит от английских слов «sex» (секс) и «texting» (переписка). Первоначально термин подразумевал электронную переписку с эротическим содержанием. С развитием технологий термин эволюционировал и теперь предполагает обмен интимными фотографиями и видео. Это стало обычной практикой, так как у большинства подростков и детей есть личные мобильные устройства.

Спам

Вы точно видели спам раньше. Это те самые «нежелательные письма», которые каждый день забивают ваш электронный почтовый ящик. Обычно эти сообщения содержат рекламные предложения, но они могут нести в себе и потенциально опасный контент.

Кража информации

Вся информация, проходящая через Сеть без необходимой защиты, может быть перехвачена третьими лицами. В большинстве случаев именно персональные данные являются целью нападения на компьютер и мобильные устройства. Один неверный шаг может привести к потере семейных денег или краже личных данных.

Есть два основных способа, с помощью которых злоумышленник может получить ваши личные данные:

- выманить информацию у ребенка с помощью методов социальной инженерии (например, притворившись его другом или сверстником);

- изучить открытый профиль у ребенка, воспользовавшись тем, что в аккаунте не настроены параметры безопасности.

Важно отметить, что это общая проблема, и даже взрослый человек может пострадать от этой угрозы.

Рекомендации

1. Используйте инструменты родительского контроля

Функции родительского контроля можно использовать как в браузерах, так и в антивирусных программах. Например, в **ESET NOD32 Smart Security** предусмотрен модуль «Родительский контроль». Кроме того, вы можете выбрать специальное мобильное приложение – **ESET NOD32 Parental Control для Android**. Существуют подобные инструменты для игровых приставок, таких как Nintendo Wii, Playstation и Xbox 360.

2. Не разрешайте детям публиковать в интернете личную информацию

Запомните и объясните детям, что конфиденциальная информация никогда не запрашивается по электронной почте или в чате. Банки никогда не требуют прислать им данные от личного кабинета или PIN-код карты. Лучше, если дети не будут иметь доступа к вашим финансовым данным.

3. Не отвечайте на оскорбительные сообщения, но и не удаляйте их

Если ваш ребенок стал жертвой кибербуллинга, он не должен отвечать на оскорбительные сообщения. Объясните ребенку, что обидчик хочет спровоцировать ответную реакцию. Если ребенок попал в такую ситуацию, обратитесь в соответствующие органы. Не удаляйте сообщения агрессора, история сообщений послужит доказательством акта запугивания.

4. Доверяй, но проверяй

Объясните ребенку, что далеко не вся информация в интернете достойна доверия. Чтобы наглядно это продемонстрировать, напишите пост в блоге или соцсети и покажите, как просто изменить его содержимое на диаметрально противоположное.

5. Ведите с ребенком открытый диалог

Ключевую роль в обеспечении безопасности детей играет общение с ними. Разговоры о безопасности, страхах и проблемах намного эффективнее наказаний. Доброжелательная атмосфера в семье и открытый диалог способствуют успешному развитию ребенка.

6. Все, что попало в интернет, останется там навсегда

Объясните детям, что информация, проиндексированная поисковыми системами, навсегда останется в Сети. Хуже того, после публикации пользователь теряет контроль над своими данными, любой может использовать и распространять эту информацию. Пусть дети возьмут за правило никогда не публиковать фотографии, статусы и другой контент, который они не хотели бы показывать родителям или родственникам. Это распространяется на соцсети, мессенджеры, блоги и другие сервисы.

7. Используйте комплексные антивирусные продукты

Чтобы избежать заражения ваших и «детских» устройств вредоносными программами, установите комплексный антивирус с поддержкой эвристических технологий. Дополнительным преимуществом является наличие функций антиспама и файервола. Не рекомендуется создавать для ребенка учетную запись с правами администратора.

8. Настройте использование https

Убедитесь в том, что ваш ребенок открывает сайты с защищенным протоколом https (наименование протокола отображается в адресной строке браузера). Это позволит избежать перехвата информации – данные передаются в зашифрованном формате, который не распознают вредоносные программы. Посоветуйте детям-подросткам использовать эти настройки и при доступе к соцсетям через публичный Wi-Fi.

9. Используйте надежные пароли и двухфакторную аутентификацию

Ваши дети знают, как выглядят надежные пароли? Убедитесь в том, что они не используют пароли, которые легко подобрать: «пароль», «12345» и пр. Надежный пароль содержит не менее десяти символов, буквы верхнего и нижнего регистров, цифры и специальные знаки («#» или «@»). Напомните детям, что пароли нельзя передавать или давать на время даже лучшим друзьям. Удостоверьтесь, что ребенок использует для входа на Facebook, Вконтакте, Twitter и другие соцсети двухфакторную аутентификацию (например, с получением кода в SMS). Эту функцию можно настроить в параметрах безопасности.

10. Настройте параметры безопасности для социальных сетей

Параметры безопасности в соцсетях, установленные по умолчанию, не гарантируют безопасности. Рекомендуется посвятить немного времени их правильной настройке и проверить, какая информация находится под угрозой утечки. Рассмотрим настройку параметров безопасности на примере наиболее популярных соцсетей:

- **Facebook и Вконтакте**

Убедитесь, что профиль ребенка не размещен в открытом доступе. Задайте возможность просмотра страницы вашего ребенка только друзьями или создайте отдельную группу друзей (для семьи и самых близких людей), если френд-лист слишком велик.
Установите ограничения просмотра фотографий, статусов и другого контента, где может быть отмечен ребенок.
Ограничьте доступ приложений к личной информации ребенка и отключите возможность публикации в его аккаунте.

Расскажите ребенку, что запросы о добавлении в друзья стоит принимать только от лично знакомых людей. Объясните, что общаться с незнакомцами в киберпространстве может быть так же опасно, как и в реальной жизни.

- **Twitter**

Социальная сеть Twitter имеет свою специфику – ограничение текста 140 символами и укороченные URL-адреса. Базовые правила безопасности: избегать подозрительных ссылок, которые могут вести на мошеннические сайты.
Кроме того, установите на компьютере и мобильном устройстве ребенка плагин для браузера, который будет показывать настоящую ссылку вместо укороченной до перехода.

5 подсказок для родителей

1. Создайте для ребенка учетную запись с правами обычного пользователя – это позволит вам эффективно контролировать его онлайн-активность. Учетная запись с правами администратора должна использоваться только взрослым.

2. Не забывайте регулярно обновлять антивирус и программу родительского контроля.

3. Просматривайте историю посещения сайтов ребенком. Если вы обнаружите, что история подчищена, найдите повод, чтобы с ребенком поговорить.

4. Проверьте настройки веб-камеры и убедитесь, что она отключена или закрыта, если в данный момент не используется.

5. Проверьте настройки профиля ребенка в соцсетях. Открытый доступ к профилю может подвергнуть ребенка риску.

P.S.

Предлагаем на всякий случай повторить простые советы по безопасности в Сети:

1. Не переходите по подозрительным ссылкам
2. Не посещайте сайты с сомнительной репутацией
3. Регулярно устанавливайте обновления операционной системы, программ и мобильных приложений
4. Скачивайте программы и мобильные приложения только из официальных источников
5. Используйте комплексные антивирусные продукты и решения
6. Избегайте заполнения сомнительных форм с персональными данными в Сети
7. Просматривайте результаты поисковых запросов, прежде чем перейти по ссылке
8. Принимайте запросы о добавлении в друзья в соцсетях только от знакомых вам лично людей
9. Не открывайте файлы от неизвестных отправителей
10. Используйте сложные неповторяющиеся пароли

Заключение

Сегодня полный запрет доступа детей к технологиям не решает проблему безопасности. Современные технологии – важная часть повседневной жизни, необходимая для развития. Вместо того чтобы устанавливать ограничения, поговорите с детьми о безопасности и организуйте взаимодействие ребенка с гаджетами. Многие вышеупомянутые риски актуальны и для взрослых, поэтому рекомендованные меры предосторожности стоит применять в любом возрасте.

Детская безопасность – ответственность взрослых. Подсказки и рекомендации, приведенные в данном руководстве, помогут вам защитить персональные данные несовершеннолетних пользователей, а также собственные финансы и «здоровье» компьютеров и мобильных устройств.

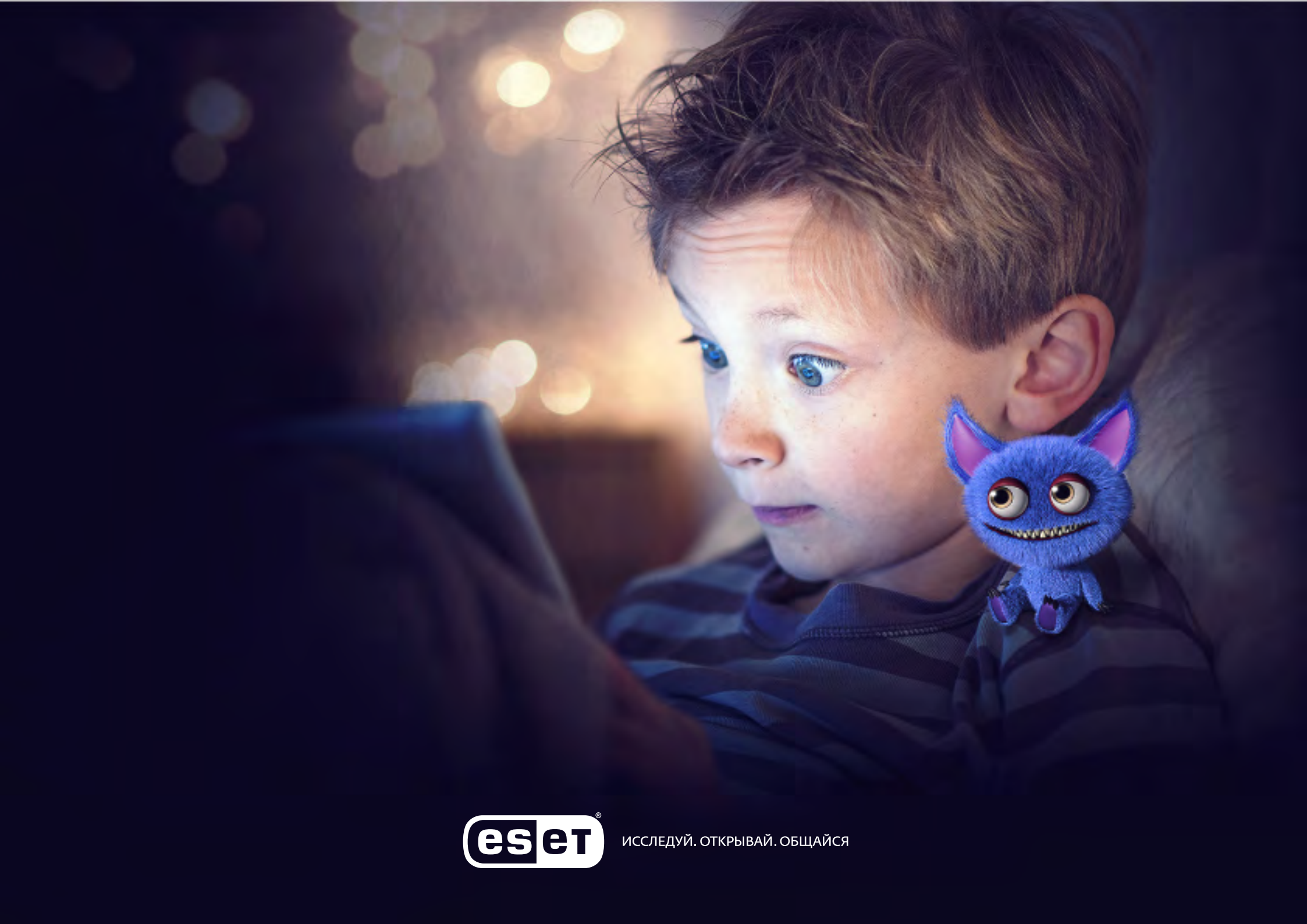
Для получения дополнительной информации посетите наш корпоративный сайт:

www.esetnod32.ru

Присоединяйтесь к нам в соцсетях:

www.facebook.com/ESETNOD32Russia
www.vk.com/nod32
www.ok.ru/nod32

Читайте нас в *www.twitter.com/ESETNOD32Russia*
Смотрите нас на *www.youtube.com/user/ESETNOD32Russia*


eset
ИССЛЕДУЙ. ОТКРЫВАЙ. ОБЩАЙСЯ