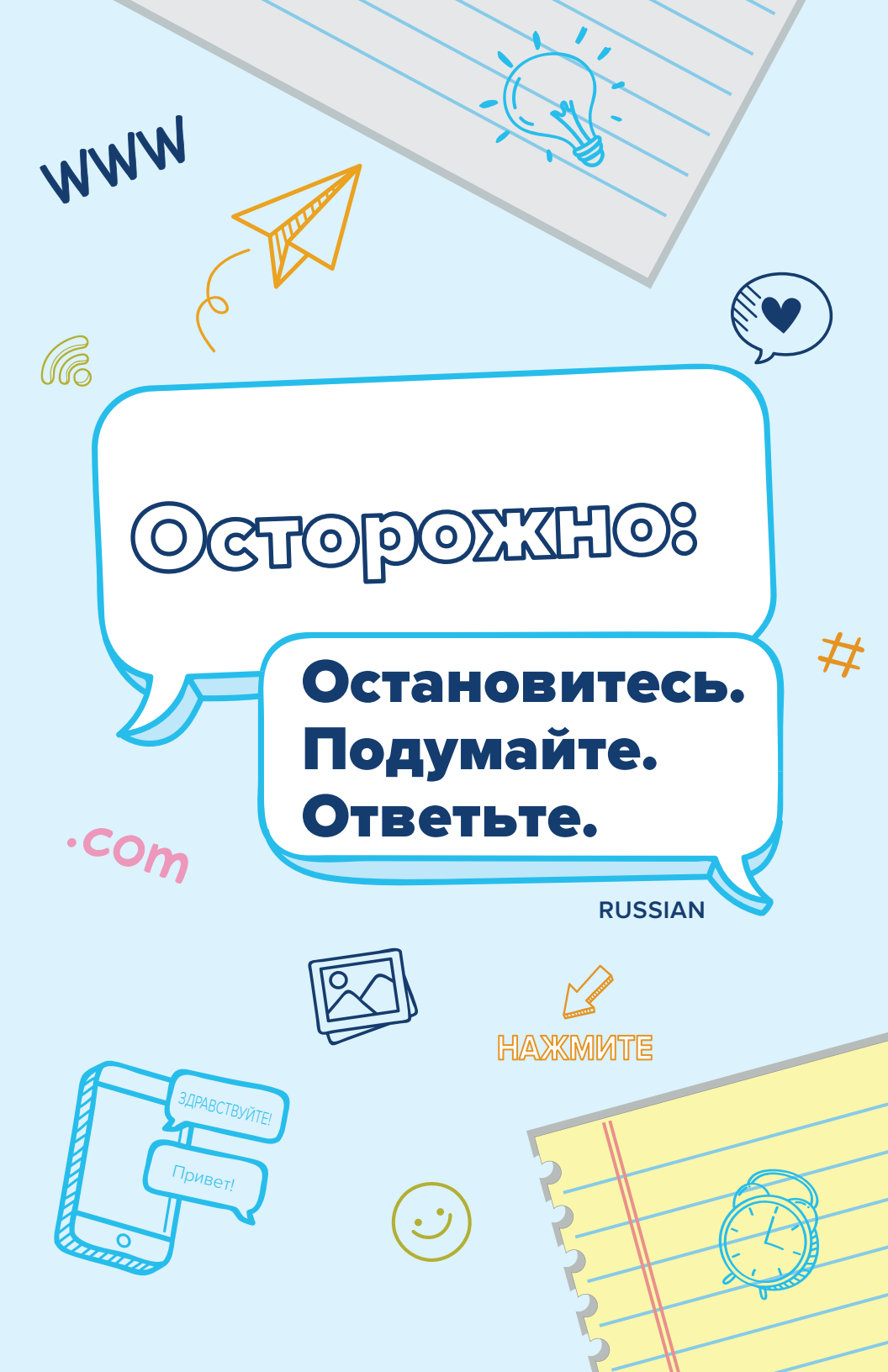
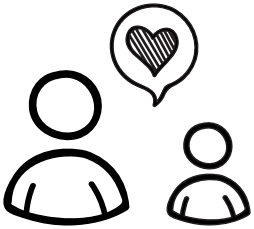

WWW
Осторожно:
Остановитесь.
Подумайте.
Ответьте.
.com
RUSSIAN
НАЖМИТЕ
ЗДРАВСТВУЙТЕ!
Привет!



Чтобы помочь вашим детям быть в безопасности в Интернете в брошюре *«Будьте осторожны: остановитесь, подумайте, ответьте»* приведены несколько идей, которые помогут вам начать с разговор с детьми. Выберите раздел и совместно прочитайте его, чтобы узнать, как делиться информацией с осторожностью, быть добрыми в сети, противостоять кибербуллингу и защищать их (и ваши) личные данные в Интернете. Эти инструменты помогут вам показать детям, как делать правильный выбор и ответственно использовать технологии. Кроме того, разговаривая с ними, вы даете детям понять, что у них есть надежный взрослый, который поможет им, если они совершат ошибку.

To help kids in your life be safe online, *Heads Up: Stop. Think. Connect.* has some ideas to help you start a conversation with them. Pick a section and read it together to see how to share with care, be kind online, stand up to cyberbullying, and protect their (and your) personal information online. These tools can help you show kids how to make good choices and use technology responsibly. And, by talking with them, you let kids know they have a trusted adult to help them when they make mistakes.

Деятельность в Интернете - это часть вашей жизни. Вы смотрите и создаете контент, публикуете фотографии и видео, играете в игры и делитесь с друзьями и близкими информацией о том, где вы находитесь и чем занимаетесь. Но когда вы публикуете материалы, играете и общаетесь в Интернете, это сопряжено с определенными рисками. Некоторые люди и ситуации, с которыми вы сталкиваетесь, не всегда такие, какими кажутся.

Независимо от того, насколько быстро ваши пальцы летают по клавиатуре, телефону или планшету, лучшие инструменты для предотвращения рисков в Интернете - это ваш мозг и время. Остановитесь и обдумайте ситуации, чтобы защитить себя, своих друзей и близких, свои учетные записи и устройства. В противном случае вы можете переборщить с обменом информацией, поставить себя или других в неловкое положение, испортить компьютер или общаться с людьми, которые не являются теми, за кого себя выдают.

- **Делитесь информацией с осторожностью**
- **Быть добрым - это круто**
- **Противодействие кибербуллингу**
- **Защищенное соединение**

Делитесь информацией с осторожностью

Подумайте, прежде чем поделиться информацией

То, что вы делаете в Интернете, имеет последствия в реальном мире. Фотографии, видео и сообщения, которыми вы делитесь, влияют на вас, вашу частную жизнь, вашу репутацию и репутацию окружающих вас людей - сейчас и в будущем. Остановитесь и подумайте, прежде чем поместить информацию на Интернет.

То, что вы публикуете, может иметь большую «аудиторию», чем вы думаете.

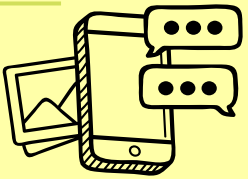
Невозможно полностью контролировать, кто видит ваш профиль, фотографии, видео или тексты - даже если вы используете настройки приватности или приложения, которые удаляют контент после просмотра или в течение 24 часов. Любой человек, который увидит ваше сообщение, может сделать снимок экрана или запись. Спросите себя: «Хотел бы я, чтобы кто-то встал посреди обеденного перерыва и поделился этой фотографией или видео со всем кафетерием?»

То, чем вы делитесь, может повлиять на других. Отправлять или публиковать фотографии и видео без разрешения людей, которые на них изображены, может быть неудобно, нечестно и даже небезопасно. Сначала получите разрешение другого лица. Перед публикацией спросите этого человека: «Вы не против, если я опубликую это в социальных сетях?» Если они скажут «нет», не публикуйте это.

Разместив что-то в Интернете, вы не сможете удалить это.

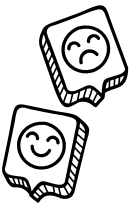
Даже если вы удалите опубликованное сообщение - или срок его действия истечет - фотография или комментарий, которые вы не хотите, чтобы люди больше видели, могут быть сохранены, распространены и жить где-то в сети - навсегда.

Секстинг: не делайте этого



Возможно, вы слышали в школе или в новостях истории о том, как люди занимаются «секстингом» - отправляют фотографии обнаженных людей со своих телефонов. Не делайте этого. Никогда. Создавая, пересылая или даже сохраняя откровенно сексуальные фотографии, видео или сообщения, вы подвергаете риску ваши дружеские отношения и репутацию. Что еще хуже, вы можете нарушить закон.

Примечание о социальных сетях



По мнению Главного санитарного врача США, использование социальных сетей может навредить вам, в зависимости от того, сколько времени вы проводите на платформах, какой тип контента вы просматриваете и насколько это мешает вам спать или заниматься спортом - теми видами деятельности, которые необходимы для вашего здоровья.

Быть добрым - это круто

Вежливость имеет значение

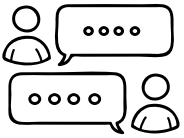
Когда вы не видите выражения лица, языка тела или других визуальных признаков человека в сети, вы можете почувствовать себя свободным и написать или сказать то, что не сказали бы при личной встрече. Но СМС, сообщения, прямые сообщения, видеоигры и электронная почта - это то же самое, что и разговор с человеком лицом к лицу. Будьте внимательны к тому, как вы общаетесь, и думайте, прежде чем говорить или размещать информацию.

Не торопитесь. При общении в Интернете легко возникают недоразумения. Прежде чем отправить сообщение, спросите себя: «Как это сообщение воспримут другие люди?»

Учитывайте и уважайте точку зрения и чувства других людей в Интернете — так же, как и при личном общении. Помните, что за аватарами и именами профилей скрываются реальные люди.

Сбавьте тон. Не используйте все заглавные буквы, длинные ряды восклицательных знаков или большие жирные шрифты. Это то же самое, что и крик.

Не помещайте все в групповой чат.
Прежде чем отправить групповое сообщение или нажать кнопку «Ответить всем» (Reply All), остановитесь и подумайте: кому нужно увидеть это сообщение?



Не выдавайте себя за другого человека

Неправильно и потенциально вредно создавать профили, комментарии или сообщения, которые будто бы исходят от кого-то другого, например от кого-то из вашего класса или учителя.

Не молчите

Если вы видите, что ваш друг публикует что-то необдуманное или небезопасное, скажите ему об этом. Вы можете уберечь своего друга от неприятностей и не дать ему опозориться. Если вы увидели в Интернете что-то неподобающее, сообщите об этом и расскажите взрослому, которому вы доверяете. В большинстве приложений и платформ есть возможность сообщить о том, что чье-то поведение является угрожающим или неуместным.

Противодействие кибербуллингу

Каждый человек заслуживает того, чтобы чувствовать себя в безопасности при ежедневном общении с другими людьми, будь то на Интернете или лицом к лицу.

Если кто-то публикует злобные комментарии, обидные мемы, постыдные фотографии или отправляет чаты или личные сообщения о вас - это буллинг. Это не нормально. Поговорите с взрослым, которому вы доверяете, чтобы получить помощь в этой ситуации и решить, как вам следует реагировать.

Если кто-то преследует вас в Интернете, вот что нужно делать:

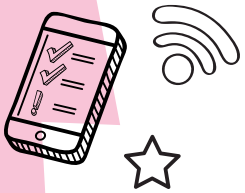
- **Игнорируйте** этого человека или заблокируйте дальнейшие контакты с ним.
- **Сохраните записи** и попросите помощи у взрослого, которому доверяете.
- **Сообщите об этом.** В большинстве приложений и платформ есть возможность сообщить о том, что чье-то поведение является угрожающим или неуместным.

Буллинг часто заставляет человека, подвергающегося преследованию, чувствовать себя плохо - и лицо, осуществляющее буллинг также выглядит плохо.

Буллинг также могут привести к неприятностям со школой или полицией.

Если вы стали свидетелем кибербуллинга, найдите способ стать защитником - тем, кто вмешивается, прерывает или высказывается, чтобы остановить буллинг. Плохое поведение обычно быстро прекращается, когда кто-то заступается за того, кто подвергается буллингу.

Защищенное соединение



Защищайте вашу конфиденциальность

Когда вы делаете что-либо в Интернете, вы оставляете за собой след. Примите следующие меры, чтобы убедиться, что этот след не приведет к информации, которой вы, возможно, не собирались делиться.

Используйте настройки конфиденциальности. Узнайте, как включить настройки конфиденциальности для устройств, приложений и учетных записей в социальных сетях, а затем сделайте это. Это поможет вам ограничить круг лиц, которые могут видеть, где вы находитесь, что вы публикуете и которые могут с вами связаться.

Проверьте настройки местоположения. Некоторые приложения позволяют видеть, где находятся ваши друзья. Они также делятся информацией о вашем местоположении. Подумайте, когда имеет смысл делиться своим местоположением. Если это не нужно, отключите доступ к местоположению. Функции вашего устройства,

например камера, могут сохранять информацию о том, где вы находились, когда делали снимок. Если вы не хотите передавать всем информацию о месте, где вы были, для каждого селфи, отключите определение местоположения на камере телефона. Всегда спрашивайте себя: «Нужно ли этому приложению знать, где я нахожусь?»

Ограничьте круг своих друзей в Интернете людьми, которых вы действительно знаете. Общение с друзьями через СМС, социальные сети или видеоигры может быть забавным, но некоторые люди оказываются не теми, за кого себя выдают в сети. И если вы не будете осторожны, то можете поделиться личной информацией с незнакомцем.

Защитите свою информацию

Если вы передадите свои личные данные - номер социального страхования, пароли или информацию о банковском счете - незнакомому человеку, вернуть их будет невозможно.

Здесь объясняется, как защитить свою информацию в Интернете:

Не отвечайте на сообщения, в которых запрашивается личная информация. Даже если сообщение выглядит так, будто оно от друга, члена семьи или знакомой компании, или в нем говорится о том, если вы не ответите, то случится неприятность. Скорее всего, это фальшивка, присланная с целью украсть ваши данные. Попросите

взрослого, которому вы доверяете, помочь вам сообщить об этом как о нежелательном сообщении или спаме.

Проверьте, к какой информации приложение хочет получить доступ, прежде чем загружать его. Некоторые приложения запрашивают разрешение на доступ к ненужной им информации или функциям, таким как список контактов, камера, хранилище, местоположение и микрофон. Попросите взрослого, которому вы доверяете, помочь вам прочитать политику конфиденциальности приложения, чтобы узнать, как будут использоваться ваши данные и будут ли они переданы. Затем решите, действительно ли этой игре в слова нужен доступ к вашим фотографиям.

Поговорите с доверенным взрослым, прежде чем совершать покупки в приложениях, особенно если они за них платят.

Защитите свои учетные записи

Вы храните много личной информации в своих учетных записях на Интернете. Вот несколько шагов, которые нужно предпринять, чтобы не предотвратить доступ других людей к вашим учетным записям.

Создайте надежные пароли.
Чем длиннее ваш пароль, тем труднее его взломать. Используйте не менее 12 символов, сочетая прописные и строчные буквы, цифры и символы. Рассмотрите возможность использования пароля в виде фразы из случайных слов, чтобы сделать ее более

запоминающейся. Но не используйте общеизвестные фразы, слова песен или цитаты из фильмов, которые легко угадать.

Пароль должен быть уникальным. Придумайте разные пароли для разных учетных записей. Таким образом, если кто-то узнает ваш пароль от одной учетной записи, он не сможет использовать его для доступа к другим учетным записям. Один из способов отслеживать все ваши различные пароли - использовать менеджер паролей.

Храните пароли в тайне. Не сообщайте свои пароли никому, даже лучшему другу или человеку, с которым вы встречаетесь.

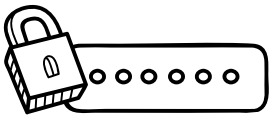
Будьте разборчивы при выборе вопросов безопасности.

Старайтесь выбирать вопросы безопасности, на которые можете ответить только вы. Не используйте вопросы с ответами, которые можно найти в Интернете - например, почтовый индекс, место рождения или девичья фамилия матери. Если вы не можете избежать этих вопросов, проявите изобретательность! Относитесь к ним как к паролям и используйте случайные и длинные ответы. Только не забудьте запомнить свои ответы.

Используйте многофакторную аутентификацию. Многие учетные записи предлагают дополнительную защиту с помощью «многофакторной аутентификации», требующей введения не только пароля, но и какой-либо дополнительной информации. Многофакторная

аутентификация сочетает в себе то, что вы знаете (например, пароль), с тем, что у вас есть (например, кодом, сгенерированным приложением), или с тем, чем вы являетесь (например, отпечатком пальца).

Быстро меняйте пароли в случае взлома.
Если какая-либо компания сообщила вам, что произошла утечка данных, в результате которой хакер мог получить ваш пароль, немедленно измените пароль, который вы используете для этой учетной записи. Также измените пароли и для всех учетных записей, использующих аналогичный пароль.



Защищайте свои устройства

Каков лучший способ получить удовольствие от пребывания в Интернете? Обеспечение безопасности и надежности ваших устройств. Начните с этого:

Установите автоматическое обновление программ безопасности для всех ваших устройств, интернет-браузеров и операционных систем. Это поможет вам защититься от новых угроз безопасности.

Не переходите по ссылкам и не открывайте вложения.
Если вы получили неожиданное СМС, электронное письмо или сообщение в Интернете, в котором вам предлагают перейти по ссылке или открыть вложение, не делайте этого! Даже если это предложение чего-либо бесплатного. В ссылках и вложениях могут скрываться вирусы или шпионские программы, которые могут испортить ваш телефон, компьютер или планшет.

Защищайте свои устройства с помощью пароля.

Это поможет уберечь ваши фотографии, сообщения и учетные записи от попадания в чужие руки.

Храните пароли в надежном месте. Не оставляйте в общественном месте телефон, ноутбук или планшет - даже на минуту.

Дополнительная информация приведена на веб-сайте

This booklet helps kids socialize safely online. There's help on how to share with care, be kind online, stand up to cyberbullying, and protect their personal information. Get free copies in English or Spanish at

ftc.gov/bulkorder

FEDERAL TRADE COMMISSION

Август 2023 г.