РЕБЁНОК, ИНТЕРНЕТ И РОДИТЕЛИ

КАК ИЗБЕЖАТЬ ЛОВУШЕК, ПОЛУЧИТЬ ПОЛЬЗУ И ОСТАТЬСЯ ДРУЗЬЯМИ?

Интернет — уникальное пространство, в котором можно найти все: от кедов и горячей пиццы до новых друзей. Мы не мыслим своей повседневной жизни без интернета. Он помогает нам в общении и в поиске информации. Удобные приложения всегда под рукой, они позволяют нам оплатить покупку или заказать товар со скидкой, посмотреть фильм или послушать музыку. Эта среда может быть настолько привлекательной, что иногда так хочется нырнуть в нее и забыть про все ограничения реального мира. И мы активно пользуемся этой возможностью.

В 2017 году каждый из нас провел в интернете почти четыре часа в день: 115 минут на компьютере и 104 минуты на мобильном устройстве.

Сегодня интернетом пользуются 80% россиян, и большинство из них это — дети и подростки.

Что дети делают в интернете?

То же самое, что и взрослые — общаются, ищут информацию, смотрят кино и мультики, слушают музыку, скачивают приложения и при этом часто разбираются во всех тонкостях гораздо быстрее нас.

Что же делают взрослые?

Как правило, они просто вручают ребенку гаджет или компьютер и надеются, что ничего страшного не произойдет.

Правильно ли это?

На самом деле, бесконтрольное использование интернета может стать причиной многих очень неприятных и даже опасных ситуаций. Психологи говорят об эпидемии интернет-зависимости. А компьютерщики — о сотнях мошеннических схем, которые подстерегают беспечного пользователя в интернете.

В этой брошюре мы:

- расскажем о рисках бесконтрольного и бездумного использования интернета;
- подскажем, как общаться с детьми на тему компьютерной безопасности;
- научим, как настроить и использовать гаджеты, сетевое оборудование и программы, чтобы избежать ловушек и угроз в Интернете.

Мнение психолога

Еще в 2009 году биолог, член Королевской академии медицины Арик Сигман в выступлении перед Европарламентом обнародовал шокирующую статистику.

Современный ребенок, которого не ограничивают в использовании интернета, к своему седьмому дню рождения проводит в виртуальном пространстве ровно 1 год.

К 18 годам «стаж» пользования Всемирной паутиной достигает 4 лет.

В то же время «радиус активности» детей, то есть площадь пространства вокруг дома, в котором они свободно исследуют окружающий мир, значительно сократился. Нынешние дети не бегают по улицам и дворам, не лазят по деревьям, не болтают друг с другом, а часами сидят, уткнувшись в смартфоны или планшеты.

Эти тенденции отрицательно сказываются на развитии мозга. Самостоятельное исследование внешнего мира стимулирует развитие независимого мышления, помогает ребенку осмыслить свои впечатления и опыт. Также оно учит ребенка делать выводы и планировать свою активность. Если вместо естественной среды детский мозг взаимодействует с интернетом, дети в буквальном смысле вырастают «оторванными от реальности».

Дети, бесконтрольно использующие интернет, не умеют адекватно оценивать риски окружающего мира, испытывают трудности в общении и не умеют сопереживать. Став взрослыми, они будут сталкиваться с проблемами и в карьере, и в личной жизни.

Время живого общения неуклонно сокращается. Растет число одиноких людей, у которых настоящую дружбу и любовь заменили «виртуальные отношения».

В 1995 году впервые был использован термин «интернет-зависимость», сегодня этот диагноз уже никого не удивляет.

Как формируется интернет-зависимость?

Психиатр Айвен Кеннет Голдберг, который ввел термин «интернет-зависимость», определил ее как «болезненное негативное стрессовое состояние, вызванное продолжительным использованием интернета».

Если сознательно не контролировать «виртуальную жизнь» детей, зависимость формируется достаточно быстро.

И вот почему:

- Социальные сети раздражают наши центры удовольствия. Мы радуемся, когда кто-то комментирует наши посты и ставит лайки фотографиям. Поэтому мы, как собака Павлова, снова и снова заходим в социальные сети, чтобы получить внимание, которого нам недостает в реальном мире.
- Интернет и социальные сети дают постоянный приток новой информации. И даже эта не очень качественная информация формирует привычку к «пережевыванию виртуальной пищи»(этот эффект можно сравнить с жеванием жвачки).
- Интернет дает нам «убежище» от реальности — пестрый контент помогает забыть о настоящих проблемах и занять мозг «пустыми» новостями.

Нас затягивает этот процесс, который со временем выходит из-под контроля. Мы заходим в интернет что-то посмотреть, но, когда через час или два «приходим в себя», даже сложно вспомнить, что именно мы искали. Знакомая картина? Однако есть вещи и пострашнее.

Ловушки виртуальной реальности

Шокирующий контент

Случайный клик по яркой картинке может привести пользователя на сайт со сценами насилия, шокирующими фотографиями или азартными играми. И если у взрослого от «нежелательного контента» может просто испортиться настроение, для ребенка такой эпизод чреват настоящей психологической травмой, слезами, истерикой, возникновением навязчивых состояний и страхов.

Кибербуллинг

Травля в виртуальном пространстве (кибербуллинг) — может начаться с пустяковой ссоры и быстро достигнуть ужасающих масштабов. У человека, который стал героем унизительных слухов, порочащих фотографий и видеороликов возникает ощущение того, что на него ополчился весь мир. Негативная информация в интернете не только мгновенно распространяется, но и навсегда остается в виде так называемого «цифрового следа». Нервное истощение или даже попытки суицида молодых людей под влиянием кибербуллинга — страшные симптомы нашего времени.

Секс и шантаж

Подростки охотно используют интернет для общения на сексуальные темы. Барьеры стыдливости падают, и когда переписка становится очень откровенной, возникает опасность сексинга — непорядочные люди могут выложить интимные послания и фотографии в открытый доступ или вымогать деньги, угрожая испортить репутацию.

Опасные знакомства

Число жертв виртуальных педофилов увеличивается с каждым годом. Попасть на крючок маньяка очень просто: все начинается с безобидной переписки, которая переходит в недвусмысленные намеки, обмен фотографиями интимного характера и провоцирует ребенка на личную встречу, которая может закончиться печально.

Только в 2017 году на горячую линию российской организации «Сдай педофила» обратилось около 400 родителей, чьи малолетние дети попались в социальных сетях на уловки педофилов.

Кража информации

Фишинг — это «выуживание» конфиденциальных данных пользователей, от адреса электронной почты до реквизитов платежных карт и сберегательных счетов. Мошенники крадут данные пользователей под различными благовидными предлогами: авторизация на сайте, необходимость «отписаться» от спама в электронной почте, оплата покупки по низкой цене или с большой скидкой, необходимость установить новое приложение. Чтобы жертва добровольно раскрыла свои персональные данные, злоумышленники могут использовать фишинговые сайты, e-mail рассылку, «поддельные сайты», всплывающие окна и рекламу.

Спам

Нежелательная почта или спам — не просто отнимает время и засоряет ваш почтовый ящик. В рассылках могут содержаться сомнительные рекламные предложения и «письма счастья», которые юный пользователь может принять за чистую монету. Кроме того, через спам можно получить компьютерный вирус или стать жертвой фишинга.

Вирусы

Загрузка сомнительных файлов или программ может привести к вирусному заражению компьютера и мобильного устройства. Вредоносные программы способны в считанные секунды полностью уничтожить программное обеспечение и даже сделать ваше оборудование частью хакерской сети. Вы даже не будете об этом знать. Вирусы маскируются под полезные программы, и распознать их без специального ПО невозможно. Отсутствие на компьютере или телефоне установленной антивирусной программы увеличивает шанс «поймать» вирус в разы.

Так что же делать?

Ведь интернет такой полезный. В нем столько удобных приложений. Там можно найти какую угодно информацию и написать любому человеку, даже если совсем его не знаешь, и он живет на другом краю планеты.

Вот только некоторые из прекрасных возможностей интернета:

- Онлайн-обучение: множество курсов, лекториев и даже виртуальных университетов дают большие возможности для самообразования и получения полезных навыков.
- Знакомство с окружающим миром, природой и обычаями разных народов: для того, чтобы совершить захватывающую виртуальную экскурсию, не обязательно уезжать из дома.
- Чтение и прослушивание книг, музыки и фильмов: интернет открывает перед вами мириады удивительных миров и дарит новые открытия каждый день.
- Общение, обмен идеями и новые знакомства: в социальных сетях и блогах можно находить близких по духу людей, делиться знаниями и идеями, вести свой блог и черпать вдохновение для творчества и развития.
- Просто отдых: в интернете можно заниматься шопингом и играть в развивающие игры, а кроме того, все самые свежие новости — тоже здесь.

Хорошая новость

Психологи советуют родителям активно участвовать в приобщении детей к интернету и принимать участие в его повседневном использовании.

Для начала самые главные правила:

- Находите время для общения с ребенком. Когда родители усаживают ребенка за компьютер, чтобы он им не мешал заниматься своими делами, они своими руками распахивают все ловушки интернета.
- Позаботьтесь о досуге своего ребенка. Чем больше у него интересов и хобби, тем больше шансов, что интернет станет для юного пользователя ценным источником информации, а на негатив просто не останется времени.
- Станьте для ребенка проводником в интернет (а не наоборот). Родителям лучше быть немного впереди собственного ребенка в области освоения Интернета. Это не просто, но стоит постараться.
- Знайте, чем ваш ребенок занимается в интернете. Добавьте его в друзья в социальных сетях и поддерживайте общение на просторах интернета. Заодно будете в курсе того, с кем он общается.

Главный ориентир — возраст ребенка

Самые маленькие пользователи (2–5 лет)

Если вы даете мобильные устройства своим маленьким детям, то обязательно предварительно настройте их так, чтобы ребенок видел только информацию, которая соответствует его возрасту.

Рассказывать малышу про угрозы интернета еще рано: он просто вас не поймет.

Действия совсем маленького ребенка проконтролировать легче всего — просто будьте рядом и посматривайте, чем он занят. Не забывайте следить за временем: слишком много интернета — вредно для здоровья ребенка.

Юные исследователи (6–11 лет)

Выпускники детского сада и младшие школьники уже делают первые самостоятельные шаги в освоении интернета. Этот возраст — самый подходящий для того, чтобы начать говорить с ребенком о компьютерной безопасности, о ловушках виртуальной реальности и необходимости дозированного использования интернета.

О чем спросить?

- Чем он интересуется в Интернете, что ищет?
- Есть ли что-то, что он не может найти?
- Какие вопросы по использованию интернета у него возникают?

Что объяснить?

- Какие источники информации являются надежными и безопасными.
- То чем делится пользователь, может стать достоянием общественности.
- Покажите разницу между реальным и виртуальным миром. Ребенок должен помнить, что не все, увиденное в интернете, является правдой — это касается и людей, и информации.

Как говорить?

Обсуждайте с юным исследователем новости, которые касаются негативного воздействия интернета на жизнь и здоровье человека.

Проявляйте максимум терпения и всегда отслеживайте реакцию ребенка на ту или иную информацию.

Спокойно и открыто выражайте свое мнение. Какую-то информацию стоит обсудить несколько раз для ее лучшего понимания.

Подростки (12+)

Подростковый возраст связан с активной социализацией — родители отходят на второй план, все большую значимость в жизни школьника получают ровесники, их кумиры и актуальные тренды молодежной среды. В это время общение с близкими взрослыми, в том числе на тему компьютерной безопасности, может стать не таким доверительным. Но подросток способен стать вашим единомышленником и соратником в борьбе за компьютерную безопасность — для этого стоит просто увлечь его этой темой.

Чему научить?

- В подростковом возрасте люди стремятся к независимости — поэтому сейчас самое время научить ребенка принимать самостоятельные решения, адекватно оценивать свою компетенцию и при необходимости обращаться за помощью.
- Подростки чаще всего заходят в интернет со своих мобильных телефонов. Подробно расскажите им об угрозах и их признаках.
- Как действовать, если он столкнулся с какой-либо опасностью в интернете.

Универсальный совет: при любых сомнениях и в любой сложной ситуации ребенок должен обратиться за помощью родителя.

Что обсудить?

- Различные виды киберугроз, их проявления и последствия для подростка и членов семьи.
- Конфиденциальность личной информации, осторожность при распространении информации о самом подростке и его близких, их имущественном положении и планах.
- Меры безопасности при интернет-знакомствах и при переходе «из виртуальной жизни в реальную».
- Настройку мобильных устройств, антивирусные программы, правила создания учетных записей и выбора пароля.

Приучайте детей через каждые 30-40 минут работы за компьютером или общения с гаджетом делать перерывы, чтобы снять напряжение с глаз, размять мышцы и немного отдохнуть.

Как говорить?

- Очень важно не давить на подростка, чтобы не вызвать отторжение. Говорите спокойно и уважительно. Будьте последовательны в ваших требованиях.
- Не ругайте подростка, если вы увидели, что он смотрит в интернете что-то неуместное. Аргументированно объясните, почему не стоит посещать подобные сайты.

Постарайтесь сделать так, чтобы компьютерная безопасность вошла в привычку у всей вашей семьи.

Дальше вы как раз найдете информацию, которая поможет вам это сделать.

Прежде, чем дать ребенку телефон или компьютер

Шаг 1. Создайте новую учетную запись на мобильном устройстве.

Эта учетная запись должна быть настроена для ребенка:

- Просмотр веб-страниц в интернете: укажите список сайтов, которые необходимо заблокировать для просмотра.
- Приложения и игры: вы можете заблокировать запуск тех или иных приложений.
- Таймер работы: задайте время, в которое ребенок сможет использовать мобильное устройство.
- Покупки и траты: позаботьтесь об отслеживании покупок ребенка в приложениях.
- Поиск ребенка: подключите полезную функцию отслеживания местоположения гаджета.

Как это сделать?

- Самое простое средство родительского контроля для Android есть по умолчанию в Google Play. Его можно настроить здесь: Google Play — Настройки — Родительский контроль. Не забудьте настроить фильтрацию контента.
- В Google Play и App Store есть возможность защиты от случайных и нежелательных покупок.
- В Google Play это можно настроить здесь: Google Play — Настройки — Аутентификация при покупке (введите пароль).
- В App Store это можно настроить здесь: Настройки — Основные — Ограничения (введите пароль для ограничений) — Включите ограничения (установка программ, удаление программ и встроенные покупки).
- В iOS есть функция «Гид-доступа», которая ограничивает использование устройства только одним приложением, при этом можно выбрать, какие функции открытой программы будут доступны. Выход из «Гида-доступа» возможен только с помощью секретной цифровой комбинации. Включить функцию можно здесь: Настройки — Основные — Универсальный доступ — Гид-доступа. Затем в активной программе нужно будет три раза нажать на кнопку «Домой», и «Гид-доступа» будет включен.

- Существуют так называемые «детские оболочки», они позволяют создавать на устройстве безопасную зону, в которой могут быть запущены только разрешенные приложения и игры. Чтобы найти такие приложения, зайдите в Google Play и в строке поиска введите запрос «детский режим».
- Существуют приложения, которые позволяют установить вход в выбранные приложения по паролю или отпечатку пальца, тем самым разграничивая доступ к ним. Чтобы найти такие приложения, зайдите в Google Play и в строке поиска введите запрос «пароль на приложения».
- Существует приложение для Android и iOS, которое позволяет ограничить время использования мобильного устройства, блокирует нежелательные сайты и приложения. Кроме того, приложение информирует о том, какие сайты посещал ребенок, какие поисковые запросы делал и определяет местоположение гаджета на карте. Чтобы найти такое приложение зайдите в Google Play или App Store и введите запрос «безопасность детей в интернете».

Шаг 2. Установите на компьютер средство родительского контроля.

Многие компании предлагают программное обеспечение, которое позволяет настроить или ограничить выход в интернет. Такие программы могут включать следующие функции:

- Фильтрация и блокировка. Позволяют ограничивать доступ к некоторым сайтам, программам и изображениям.
- Блокировка данных, которые ребенок отправляет с компьютера. Не позволяет детям делиться информацией в Интернете, в том числе отправлять что-то по электронной почте.
- Браузеры для детей. Позволяют фильтровать контент, который видит ваш ребенок.
- Поисковые системы для детей. Ограничивают поиск и фильтрует его результаты.
- Мониторинг деятельности ребенка в браузере. Организует контроль доступа детей в Интернет. Фиксирует адреса веб-сайтов, которые посещал ребенок, отправляет родителям сообщения в тот момент, когда ребенок заходит на запрещенный сайт.

Как это сделать?

Самое простое средство родительского контроля в **Windows** есть по умолчанию. Чтобы его настроить:

- создайте новую учетную запись (Параметры — Учетные записи — Семья и другие люди — Добавить пользователя для этого компьютера);
- настройте ее (Параметры — Учетные записи — Семья и другие пользователи — Управление семейными настройками через Интернет);
- в разделе «Просмотр веб-страниц» включите блокировку нежелательных веб-сайтов или укажите список доступных и недоступных сайтов;
- в разделе «Приложения, игры и мультимедиа» ограничьте доступ к выбранным программам;
- в разделе «Таймер работы с устройством» ограничьте время работы за компьютером.
- Самое простое средство родительского контроля на устройствах Apple есть по умолчанию. Чтобы его настроить:
- зайдите в «Родительский контроль» (Системные настройки — Родительский контроль), создайте новую учетную запись с родительским контролем и настройте ее;
- на вкладке «Программы» запретите или разрешите использовать камеру, ограничьте список разрешенных контактов в почте и разрешите использовать определенные программы;
- на вкладке «Веб» разрешите доступ к некоторым сайтам;
- на вкладке «Магазины» отключите встроенные магазины Apple, а также ограничьте просмотр фильмов и прослушивание музыки iTunes;
- на вкладке «Время» ограничьте время работы за компьютером.

В браузере **Google Chrome** можно включить функцию «Родительский контроль». Для этого создайте новый пользовательский аккаунт (Google Chrome — Настройки — Пользователи — Добавить нового пользователя). При создании поставьте галочку «Контролируемый профиль, управляемый пользователем», и настройте аккаунт.

В поисковой системе **Яндекс** можно исключить из результатов выдачи интернет-ресурсы с нецензурными словами и «взрослым» контентом. Для этого: зайдите на страницу поисковой системы, выберите ее настройки (Настройки — Настройки портала) и раздел «Результаты поиска». В меню «Фильтрация страниц» выберите настройку «Семейный поиск».

Шаг 3. Научите ребенка создавать надежные пароли

Расскажите детям основные правила создания паролей:

- пароль должен состоять не менее, чем из 6 символов;
- в состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы (точки, запятые, восклицательные знаки и т.д.);
- рекомендуется составлять пароль из смешанного набора цифровых и буквенных символов;
- не следует использовать общеупотребляемые слова и устойчивые словосочетания;
- не следует использовать наборы символов, представляющие собой комбинации клавиш, расположенных подряд на клавиатуре, например, такие как: qwerty, 123456789, qazwsx и т.п;
- не следует использовать персональные данные: имена и фамилии, адреса, номера паспортов, страховых свидетельств и т.п;
- для разных учетных записей необходимо использовать разные пароли.

Как это сделать?

Существуют бесплатные и довольно простые в использовании программы для создания и хранения паролей. Найдите такую программу в интернете, установите ее, создайте пароль и сохраните его.

Шаг 4. Установите антивирусную программу

Вирусы могут нанести непоправимый вред информации, хранящейся на вашем компьютере и мобильном устройстве.

Антивирусная программа — основное средство защиты компьютера и мобильного устройства от вирусов. Поэтому ее нужно обязательно установить на каждое устройство, имеющее выход в интернет.

Новые вирусы появляются каждый день, поэтому антивирусные программы необходимо регулярно обновлять.

Почти у любой антивирусной программы есть выборочная проверка — с ее помощью вы можете проверить любой файл.

Шаг 5. Защитите свою домашнюю сеть

Новые маршрутизаторы поставляются со стандартными сетевыми именами (SSID) и паролями. Эту информацию можно использовать только при первом подключении к Интернету. Затем обязательно измените сетевое имя и пароль, чтобы злоумышленники не могли получить доступ к роутеру.

Придумайте безопасный пароль и уникальное имя для своей Wi-Fi-сети.

Современные роутеры поддерживают различные методы шифрования данных, передаваемых по беспроводной сети, в том числе WEP, WPA и WPA2. WPA2 является оптимальным с точки зрения надежности.

Настройки роутеров позволяют фильтровать доступ к сети по уникальным идентификаторам устройств (MAC-адресам). Вы можете создать список MAC-адресов доверенных устройств либо запретить подключение устройств с конкретными адресами.

Не существует идеальных технологий. Злоумышленники постоянно находят новые уязвимости. Периодически обновляйте прошивку своего роутера, чтобы защититься от вторжений злоумышленников.

Некоторые маршрутизаторы имеют встроенное средство от сетевых атак — файрвол. Поищите в настройках безопасности роутера функцию с названием типа Firewall, «Брандмауэр» или «Сетевой экран» и включите ее, если

это возможно. Дополнительные параметры файервола настройте в соответствии с официальной инструкцией или обратитесь за помощью к специалисту.

Большинство домашних роутеров и беспроводных точек доступа имеют функцию ограничения доступа в Интернет в определенные часы. Поэтому вы можете ограничить возможность использования Интернета для членов семьи, не имеющих устройств с выходом в интернет и функцией модема.

Шаг 6. Не используйте открытые Wi-Fi-сети

Найти бесплатную Wi-Fi-сеть просто: едва начав поиск, вы наверняка наткнетесь на парочку. Без них сложно представить аэропорт, вокзал и другие общественные места. Чаще всего эти сети бывают открытыми, то есть доступ к ним может получить каждый.

Если у вас недорогой мобильный интернет, то лучше используйте его, а не открытые Wi-Fi-сети, так как они небезопасны.

Расскажите детям, чем опасны открытые Wi-Fi-сети:

- Анализ трафика. Владелец Wi-Fi-сети или человек, который получил к ней доступ, может просматривать весь проходящий через нее трафик. С помощью анализатора пакетов данных он может узнать, на какие страницы вы заходили с подключенных устройств и какие данные вводили.
- «Фальшивые» страницы для кражи паролей. При подключении к Wi-Fi в общественном месте пользователю часто предлагают подтвердить свою личность по номеру телефона или зарегистрироваться через соцсети. Все введенные при этом данные, владелец точки может собирать для личного использования. Также человек, у которого есть доступ к управлению роутером, имеет возможность настроить фишинг: например, перенаправление с facebook.com на сайт facebook10k.com, на котором будет размещена копия главной страницы популярной соцсети, созданная для кражи паролей.
- Заражение вредоносными программами. Пользователя открытой сети можно незаметно для него перенаправить не только на фишинговые сайты, но и на страницы для скачивания троянов и вирусов, которые могут похитить с компьютера множество ценной для мошенников информации (пароли, документы и т.д).

Шаг 7. Настройка безопасности в социальных сетях

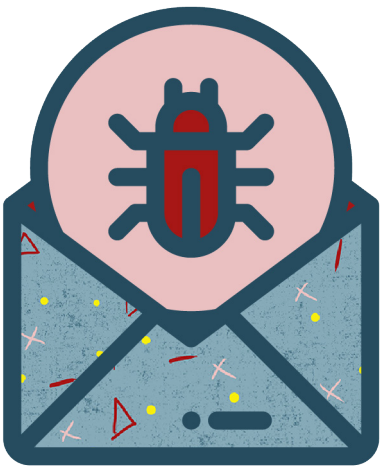
Позаботьтесь о том, чтобы в социальных сетях ребенка были установлены максимально строгие настройки безопасности.

Например, страница «В контакте» должна быть открыта только для тех, кого ребенок добавил в друзья, и писать ему сообщения могут тоже только друзья.

Шаг 8. Не читайте спам-письма

Научитесь сами и научите своих детей распознавать спам-письма.

Главные признаки спам-писем



- **Незнакомый адрес отправителя**
- **Неуместный стиль письма**
- **Информация, которую вы не запрашивали**
- **Подозрительные уведомления**
- **Отправитель и тема письма не соответствуют друг другу**
- **Подозрительная ссылка и вложенные файлы**

Универсальной защиты от угроз не существует. Поэтому самый лучший способ уберечь ребенка от этого — участвовать в его «виртуальной жизни» и приучать его к соблюдению правил компьютерной безопасности.

Посидите рядом, когда он играет в игры, посетите его любимые сайты, обсудите интересующие ребенка темы. Пусть ваш ребенок познакомит вас со своими виртуальными друзьями.

Расскажите ребенку о различных ситуациях, которые происходили с людьми в интернете. Ребенку значительно проще понять на примерах, как интернет может навредить ему.

Чего категорически нельзя делать в интернете?

Эти правила интернет-безопасности нужно соблюдать всем и каждому:

- Не сообщайте никому пароли от учетных записей в социальных сетях.
- Никогда не пересылайте пароли и личные данные по электронной почте или через мессенджер.
- Не переходите по подозрительным ссылкам, которые получаете по электронной почте, в мессенджерах и социальных сетях.
- Не вводите личные данные в любые формы, размещенные в интернете, если вы не уверены, что это необходимо. Например, сайт авиакомпании может потребовать у вас персональные данные включая данные паспорта, но вы должны быть на 100% убеждены в том, что это требование адекватно решаемой задаче.
- Не отвечайте на сообщения незнакомых людей, которые приходят вам в социальных сетях, мессенджерах и по электронной почте.
- Не вводите номер своей банковской карты на сомнительных сайтах в интернете. Предупредите детей, чтобы они без вашего разрешения не оплачивали что-либо в интернете.
- Не хвастайтесь, не пишите и не выкладывайте фотографии содержащие непосредственную информацию о доходах, дорогих покупках и отъездах на длительный срок.
- Без нужды не публикуйте в интернете данные о своем местоположении, чтобы злоумышленники не смогли отследить ваши перемещения и понять, например, когда вы уехали из дома и, что можно наведаться к вам в квартиру.
- Без нужды не публикуйте в интернете свой e-mail и номер телефона.

Помните! Интернет грозит неприятностями беспечным пользователям и приносит пользу тому, кто заботится о своей интернет-безопасности.

Как нужно вести себя в интернете?

Часто в интернете человек ведет себя иначе, чем в реальной жизни, не только из-за незнания правил поведения, но и потому, что интернет снимает психологические барьеры, ограничивающие выражение эмоций.

Американский психолог Джон Сулер назвал это «эффектом растормаживания в Сети». Интернет способствует потере идентичности и ощущению невидимости.

Но анонимность пользователя иллюзорна. Надо помнить, что найти человека, который написал что-то в интернете, не сложно.

Поэтому нужно соблюдать определенные правила поведения:

- Помните, что в интернете вы скорее всего общаетесь с живыми людьми. Придерживайтесь тех же стандартов поведения, что и в реальной жизни.
- Общаясь в интернете, будьте дружелюбны и вежливы.
- Пишите и говорите только то, что могли бы сказать собеседнику лично.
- Берегите свою репутацию.
- Всегда перечитывайте и перепроверяйте то, что собираетесь опубликовать.
- Критично относитесь ко всему написанному в интернете. Помните, что даже «Википедия» часто ошибается, так как тексты в ней пишут обычные люди. В ней довольно часто попадаются искаженные факты и спорные оценки.
- Научитесь доверять своему опыту. Если что-нибудь в интернете будет вызывать у вас психологический дискомфорт, то это стоит как можно быстрее прекратить. А детям нужно рассказать родителям о любой такой ситуации.

Интернет — не идеальное пространство, а отражение общества: самое высокое и прекрасное соседствует здесь с негативом и рисками.

Но мы знаем, что хоть интернет и является платформой для огромного количества мошеннических схем, бояться этого не стоит. Надо всего лишь научиться правильно его использовать и научить этому своих детей.