

25 = 750  
4 зм. 25 м = 150

# ПАМЯТКА

## ИНТЕРНЕТ- БЕЗОПАСНОСТЬ ДЛЯ РОДИТЕЛЕЙ

*В ногу с детьми в интернете*

Памятка разработана МБОУ ДОД «Дом детского творчества Первомайского района города Ижевска» и опубликована по инициативе Межведомственной комиссии по обеспечению профилактики правонарушений муниципального образования «Город Ижевск», Комиссии по делам несовершеннолетних и защите их прав при Администрации города Ижевска в рамках реализации Федерального закона от 23 июня 2016 г. N 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»



Проблема безопасности детей в сети Интернет уже не кажется такой далекой. Никто не может отрицать, что на сегодняшний день она встала особенно остро.

Известно, что подростки в период заниженной самооценки ищут поддержки среди своих друзей, а не в семейном кругу. Старшие подростки, желая независимости, отождествляют себя с определенной группой и склонны сравнивать ценности своей семьи и своих товарищей.

#### ЧТО ДЕЛАЮТ ПОДРОСТКИ ОНЛАЙН?

В интернет подростки загружают музыку, используют мгновенные сообщения, электронную почту и играют в онлайн-игры. С помощью поисковых серверов подростки находят информацию любого содержания и качества в сети Интернет. Большинство подростков регистрируются в частных чатах и общаются на любые темы, выдавая себя за взрослых. Ребята в этом возрасте предпочитают все, что выходит за рамки дозволенного: брутальный юмор, насилие, азартные игры, эротические и порно сайты. Девушкам, которые имеют заниженную самооценку, нравится размещать провокационные фото, они склонны на флиртоватые разговоры, выдавая себя за взрослых женщин, в результате чего становятся жертвами сексуальных домогательств.

#### СОВЕТЫ РОДИТЕЛЯМ

Поговорите со своими детьми о друзьях, с которыми они общаются онлайн, узнайте, как они проводят досуг и чем восхищаются.

Интересуйтесь, какие веб-сайты они посещают и с кем разговаривают.

Изучите программы, которые фильтруют получения информации из Интернета, например, Родительский контроль в Windows.

Наставляйте на том, чтобы ваши дети никогда не соглашались встречаться со своим онлайн-другом без вашего согласия.

Научите своих детей никогда не предоставлять личную информацию о себе и своей семье электронной почтой и в разных регистрационных формах, предлагаемых владельцами сайтов.



Контролируйте информацию, которую загружает ребенок (фильмы, музыку, игры и т.д.).

Интересуйтесь, не посещают ли ваши дети сайты с агрессивным содержанием.

Научите своих детей ответственному и этическому поведению онлайн. Они не должны использовать Интернет сеть для распространения сплетен, у других людей и хулиганских действий.

Убедитесь, что дети консультируются с Вами относительно любых финансовых операций, осуществляя заказ, покупку или продажу через интернет.

Информируйте детей относительно потенциального риска при их участии в любых играх и развлечениях.

Разговаривайте с ребенком как с равным партнером, демонстрируя заботу об общественной морали.

Используя эти рекомендации, Вы имеете возможность максимально защитить ребенка от негативного влияния всемирной сети Интернет.

Но помните, Интернет – это не только очаг негативной информации и стокости, но и самая богатая в мире библиотека знаний, развлечений, общения и других полезных вещей. Вы должны научить своего ребенка правильно пользоваться этим неисчерпаемым источником информации.

**НО САМОЕ ГЛАВНОЕ: РЕБЕНОК ДОЛЖЕН ПОНИМАТЬ, ЧТО ВЫ ЛИШАЕТЕ ЕГО СВОБОДНОГО ДОСТУПА К КОМПЬЮТЕРУ, А, ПРЕЖДЕ ВСЕГО, ОБЕРЕГАЕТЕ.**

#### РЕБЕНОК ДОЛЖЕН ВАМ ДОВЕРЯТЬ!

Многие дети гораздо лучше владеют компьютером, чем их родители. Однако, они по-прежнему нуждаются в советах и защите при использовании интернета и мобильных технологий.

1. Более 40% детей сталкиваются с сексуальными изображениями в интернете.

2. 80% школьников имеют аккаунты в социальных сетях.



3. 70% в своих аккаунтах указывают свою фамилию, точный возраст и номер школы.
4. 40% российских детей готовы продолжить онлайн - общение в реальной жизни.
5. У 30% школьников данные аккаунта открыты всему миру.
6. Более 20% детей становятся жертвами нападков со стороны сверстников.
7. Младшие школьники сталкиваются с сексуальными изображениями реже, чем старшие, но испытывают больший стресс.
8. Прилежные дети в 2 раза чаще попадают на «плохие» сайты в силу природной любознательности.

### ВНИМАНИЕ!!!

**Никогда** не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.

Используйте нейтральное экранное имя, не содержащее непристойных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.

**Выключите** компьютер, если вас что-то пугает в его работе. Расскажите об этом родителям или другим взрослым.

**Всегда** сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас сомнение или тревогу.

Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.

**Никогда** не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.

**Прекращайте** любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие непристойные намеки. Расскажите об этом родителям!



### ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ЕСТЬ ЛИ ОНА У ВАШИХ ДЕТЕЙ?

То, что дети проводят в Интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветствовали появление Сети, полагая, что она - безграничный источник новых знаний. Вскоре выяснилось, подростки не столько пользуются Интернетом для выполнения домашних заданий или поиска полезной информации, сколько общаются в чатах и играют в онлайн-игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями всегда было испытанием для родителей. Интернет сделал это еще более трудной задачей. Общение в Интернете и интерактивные игры могут настолько затягивать детей, что они часто теряют ощущение времени.

### ПРОФИЛАКТИКА ИНТЕРНЕТ-БЕЗОПАСНОСТИ.

1. Обратите внимание на психологические особенности вашего ребенка. Социально неадаптированные дети имеют повышенную вероятность к пристрастию Интернет-зависимости.

Причина в том, что Интернет позволяет им оставаться анонимным, не испытывая осуждения, предоставляет гораздо более широкий выбор возможностей общения, чем реальный мир.

В Интернете ребенку гораздо легче выстроить свой виртуальный мир, пребывание в котором ему будет комфортно. Поэтому, если у ребенка что-то получается в реальном мире, он будет стремиться к пребыванию там, где ему комфортно. С другой стороны, Интернет может помочь застенчивому ребенку стать более общительным, найти ту среду общения, которая более полно соответствует его уровню развития, и в результате повысить его самооценку. Если ваш ребенок в жизни замкнут, застенчив или склонен к унынию, вам необходимо внимательно следить за его отношением к Интернету, с тем чтобы предотвратить его превращение из средства раскрытия личности ребенка в плохо контролируемую страсть.

2. Следите за симптомами проявления Интернет-зависимости. Она проявляется в том, что дети до такой степени предпочитают жизнь в Интернете, что фактически начинают отказываться от своей реальной жизни, проводя



виртуальной реальности большую часть своего времени. Интернет-зависимый ребенок чаще всего тих и замкнут, он ждет не дожидается, когда можно будет подключиться к Интернету, ему тяжело выйти из него, он впадает в депрессию или становится раздражительным, если на несколько дней его отлучили от Интернета.

**3. Спросите себя:** оказывает ли времяпровождение в Сети влияние на школьные успехи вашего ребенка, его здоровье и отношения с семьей и друзьями?

**4. Выясните, сколько времени ваш ребенок проводит в Интернете.**

**5. Обратитесь за помощью к специалистам.** Если у вашего ребенка проявляются серьезные признаки Интернет-зависимости, проконсультируйтесь с педагогом или психологом. Навязчивое использование Интернета может быть симптомом других проблем, таких, как депрессия, раздражение или низкая самооценка. И когда эти проблемы будут решены, зависимость от Интернета может пройти сама собой.

**6. Не запрещайте Интернет.** Для большинства детей он является важной частью их общественной жизни.

**7. Установите «Внутрисемейные правила использования Интернета».** Ограничьте количество времени, которое ежедневно проводит в Интернете ребенок; запрет на Сеть до выполнения домашней работы; ограничьте посещение чатов или просмотр материалов «для взрослых».

**8. Поддерживайте равновесие.** Пусть ребенок почаще играет с другими детьми на свежем воздухе. Помогите ребенку участвовать в общении вне Интернета. Поощряйте участие ребенка в тех видах деятельности, которые объединяют детей с одинаковыми интересами, например, судомодельный или литературный кружок.

**9. Контролируйте своих детей.** Существуют программы, которые ограничивают использование Интернета и осуществляют контроль за тем, какие сайты посещаются. Однако сообразительный ребенок, если постарается, может отключить эту службу. Ваша конечная цель - развитие у детей самоконтроля, дисциплины и ответственности.



**10. Предложите альтернативы.** Если вам кажется, что ваши дети интересуются только онлайн-игровыми развлечениями, попробуйте предложить им альтернативный аналог одной из их любимых игр.

**Следите за достижением равновесия у вашего ребенка между временем, проводимым в Интернете и вне его!**

### БУЛЛИНГ:

При кажущейся существенной разнице между виртуальным и реальным мирами на первый взгляд, при более детальном рассмотрении оказывается, что сходств между ними не больше, чем различий. Например, в сети Интернет тоже есть свои хулиганы.

### ЧТО ТАКОЕ КИБЕРБУЛЛИНГ?

Первый случай кибербуллинга был зафиксирован в 2002 году. Американский подросток Жислен Раза ради развлечения снял видеоролик, в котором, подобно герою фильма «Звездные войны», фехтовал бейсбольной битой вместо лазерного меча. Одноклассники разместили в сети это видео с целью позабавиться над Жисленом. Эту запись просмотрели миллионы людей, через несколько дней был создан специальный сайт с исходным видео и пародиями на него. Насмешки сломали психику Жислена Раза, и его родители были вынуждены обратиться к психиатру.

Спектр целей кибер-преследователей широк, но всех объединяет стремление нанести жертве психологический ущерб. Это могут быть шутки, которые просто уязвят жертву, а могут быть психологический террор, который приводит к суициду.

### ОСНОВНЫЕ ВИДЫ КИБЕРБУЛЛИНГА.

- Флейм (от английского «flame») или виртуальная перепалка.
- Обмен эмоциональными репликами в открытом доступе. Вначале все воспринимается как активное обсуждение, но оно может зайти дальше и нанести человеку психологический вред.
- Атаки
- Буллинг по сотовой связи сводится к отправке жертве повторяющихся оскорбительных сообщений или звонков.



- На форумах и в чатах преследователи понижают авторитет жертвы, если такая форма ранга предусмотрена на форуме.
- Оказывают давление в обсуждениях, реагируют на сообщения жертвы унижающими и оскорбительными сообщениями и совместным обсуждением реальных и мнимых недостатков жертвы. Обычно этим занимается целая группа преследователей.
- В онлайн - играх преследователи играют не ради победы, а с целью понизить игровой опыт жертвы целенаправленным давлением.
- Клевета. Распространение оскорбительной и неправдивой информации в виде фото, сообщений, песен. Нередко это может быть не отдельная жертва, а целая группа подростков, которые попадают под критику и шутки одноклассников.
- Самозванство. Преследователь представляется жертвой: или используя доступ к ее аккаунту, или создавая фейк (фальшивый аккаунт). От имени жертвы распространяет в блогах, социальных сетях и системах мгновенных сообщений негативную информацию, провоцируя окружающих на конфликт с жертвой.
- Распространение закрытой информации. Получив конфиденциальную информацию о жертве, преследователь передает ее тому, кому она не предназначалась, вызывая конфликт.
- Изоляция. Любому человеку присуще желание быть частью общества (класса, группы подростков во дворе, в сообществе в социальной сети). Изоляция человека от общества наносит серьезную травму человеку. Формы изоляции в киберпространстве могут быть разными, начиная от создания закрытого сообщества до игнорирования сообщений жертвы.
- Киберпреследование. Скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.
- Хеннислеппинг («Happy Slapping» с английского «счастливое похлопывание»). Заключается в избиении жертвы и с записью этого на видео, с последующим выкладыванием ролика в сети. Подобные ситуации не редкость в новостях по телевизору.



### КАК ВЫРАБОТАТЬ ИММУНИТЕТ?

Не бросайтесь в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если вы начнете отвечать оскорблениями на оскорбления, то только еще больше разожжете конфликт.

Управляйте своей киберрепутацией. Анонимность в сети мнимая, так что в случае нанесения реального вреда, найти злоумышленника можно.

Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все ваши действия и сохраняет их. Удалить их будет крайне затруднительно.

Соблюдайте свою виртуальную честь смолоду. Храните подтверждения фактов нападений. Сохраняйте или распечатайте страницу. Игнорируйте единственный негатив. Обычно агрессия прекращается на начальной стадии. Лучшая защита от нападения - игнорирование.

Бан агрессора. В программах обмена мгновенными сообщениями в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

Не стоит игнорировать агрессивные сообщения, если они содержат угрозы, особенно систематические. Следует скопировать эти сообщения и обратиться в правоохранительные органы. По поводу размещения оскорбительной информации, размещенной на сайте, следует обратиться к администратору с требованием ее удаления.

### ИНФОРМАЦИЯ В СЕТИ

Пятьдесят лет назад объём информации, созданный человеком, был в 100 000 раз меньше того, что обрушивается на нас сегодня. И этот информационный вал увеличивается каждый с 1990 года в два раза за год, а уже сейчас учёные говорят об удвоении за несколько месяцев. Запоминать информацию, как это было раньше, просто физически неспособен человеческий мозг. Основным навыком цифрового человека становится не умение запоминать, а умение искать.



Бичом digitalhomo стал информационный перегруз. При определённом объёме поступающей информации человеческий мозг перестаёт справляться и включает защитный механизм. Это отражается на поведении человека, он перестаёт глубоко вникать в суть информации, фильтрует информацию, откладывает анализ на позднее время и т.д. Более существенным последствием информационного перегруза является формирование клинового мышления. Это когда в голове представление об объекте представляет последовательность слабосвязанных образов. Это синдром еще называют «тугозависимостью». DigitalHomo просто необходимо соблюдать информационную диету.

### ПОИСКОВЫЙ СПАМ

Интернет содержит огромное количество информации и, к сожалению, часть этой информации является информационным мусором.

Причин возникновения информационного мусора несколько.

Чтобы повысить сайт в поисковой выдаче их владельцы создают мусорные страницы, тексты со ссылками на основной сайт. Иногда на одну страницу ведут тысячи мусорных страниц с других сайтов.

Выглядит иногда это так. Набирая поисковый запрос в Яндекс или Google, вам предлагается список сайтов, содержащих эти слова. Этот список называется поисковая выдача. Но заходя на эти сайты, ценной информации вы не обнаруживаете. В чем причина?

Администраторы сайтов, чтобы обмануть поисковые системы, наполняют сайт ключевыми словами, которые люди набирают в поиске. Повторений этих слов много - значит сайт содержит информацию данной тематики, так считает поисковик и выдает вам этот сайт. Все, конечно, сложнее, поскольку поисковые системы борются с такими сайтами, контролируя как долго находится посетитель на данном сайте и переходит ли на другие страницы. Существует еще много подобных инструментов, но поисковики держат их в секрете, чтобы администраторы сайтов не придумали новый обман пользователей.

Много ли таких сайтов с поисковым мусором? Много, почти половина интернета, если не больше.

### УПРАВЛЯЕМАЯ ИНФОРМАЦИЯ

Иногда заведомо ложная информация (фейк) разносится с умыслом повлиять на общественное мнение. Вы слышали об армиях ботов? Создаются целые подразделения, которые ежедневно «постят» десятки тысяч комментариев в социальных сетях и на форумах, рассылают информации в автоматическом режиме десятками миллионов сообщений. Цель этих действий одна - сформировать иное общественное мнение, повлиять на стабильность в государстве, а иной раз совершить даже государственный переворот.

Управляют мнением пользователя сети и проще, например, мигающие баннеры с кричащими названиями, вроде «Найден секретный рецепт фараона» или «Она рассказала тайну своего рождения» и это тоже «управляемая информация».

### ВРЕДНЫЙ КОНТЕНТ

Вам нравится насилие или оскорбления в реальном мире? Разумеется, нет. Как же защититься от негативной информации в сети?

▪ Реестр запрещенных сайтов. Сайты, содержащие порнографию с детьми, пропаганду и продажу наркотиков, экстремистский контент, призывающие совершению самоубийств, включают в специальный реестр, который раскрывается провайдером. Провайдер на своем оборудовании закрывает просмотр этих сайтов для своих клиентов.

Причины такого технологического решения различны, но основная причина в том, что если такой сайт-нарушитель размещался бы в рунете, т.е. на серверах, расположенных в Российской Федерации, его можно было бы закрыть решением суда. В большинстве своем подобные сайты находятся вне юрисдикции Российской Федерации, где закрыть их очень сложно. По этой причине просто блокируется просмотр этих сайтов.

▪ Поисковики Яндекс и Google предоставляют опции безопасного поиска который исключает из выдачи вредный контент.

▪ В учебных учреждениях стоят фильтры, которые также закрывают просмотр вредный контент.

▪ Родителям доступны программные обеспечения или опции провайдеров, которые получили название «Родительский контроль», так же позволяющие оградить детей от вредного контента.

### ЛИЧНЫЕ ДАННЫЕ

Личные или персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу.

### ЧТО ВКЛЮЧАЮТ В СЕБЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

В Федеральном законе № 152-ФЗ «О персональных данных» под персональными данными подразумевают любую информацию, которая позволяет



определить личность пользователя. То есть это фамилия, имя и отчество, дата и место рождения, адрес, семейное положение, паспортные данные, профессия, доходы и другая информация. При этом пароли к аккаунтам не являются персональными данными, так как не сообщают ничего о человеке.

С согласия пользователя данные могут становиться общедоступными — например, номер телефона или e-mail, которые вы передаёте компании. При этом по требованию пользователя эти данные должны быть убраны из общего доступа.

### КАК ПЕРЕДАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

За свободный интернет и бесплатные сервисы пользователи платят данными. Крупные компании вроде Google и Яндекса синхронизируют информацию из различных источников, чтобы точнее определить предпочтения пользователя. Они зарабатывают на рекламе, и чем понятнее будут интересы пользователя, тем более точное объявление можно ему показывать. Так, в Facebook пользователям предлагают спонсируемые истории, исходя из страниц, которые ему нравятся, и оставленной информации в публичном доступе (в его профиле).

Рейтинговые системы, вроде Pluso или Liveinternet, приносят компаниям больше знаний о пользователях, которые можно анализировать и продавать для создания рекламы. Когда пользователь обращается к сервису, он принимает условия соглашения, где прописаны условия обращения с его данными. Мы передаём данные каждый раз, когда авторизуемся в сервисе, и показываем своё поведение, переходя по страницам и нажимая лайки.

### ФАКТЫ!

- 47 миллионов пользователей заходят на сайт «ВКонтакте» каждый день. Они могут увидеть информацию о вас.
- 80% преступников берут информацию в социальных сетях.
- Личная информация используется для кражи паролей.
- Личная информация используется для таких преступлений, как шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение.

### СПОСОБЫ ЗАЩИТЫ

- При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник);
- Необходимо настроить приватность в социальных сетях и других сервисах;
- Не публикуйте информацию о своем местонахождении и (или) материальных ценностях;
- Хорошо подумайте, какую информацию о себе вы хотите опубликовать в Интернете;

- Не доверяйте свои секреты незнакомцам из Интернета;
- Создайте отдельную электронную почту для регистрации в социальных сетях;

**ВСЕ, ЧТО ПОПАЛО В ИНТЕРНЕТ, ОСТАЕТСЯ ТАМ НАВСЕГДА!**

**ПОМНИТЕ: ЗА ВИРТУАЛЬНЫЕ ПРЕСТУПЛЕНИЯ ОТВЕЧАЮТ РЕАЛЬНОМУ ЗАКОНУ!**

- Статья 146 УК РФ - Нарушение авторских и смежных прав;
- Статья 159.6 УК РФ - Мошенничество в сфере компьютерной информации;
- Статья 165 УК РФ - Причинение имущественного ущерба путем обмана или злоупотребления доверием;
- Статья 242 УК РФ - Незаконное изготовление и оборот порнографических материалов или предметов;
- Статья 242.1 УК РФ - Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних;
- Статья 272 УК РФ - Неправомерный доступ к компьютерной информации;
- Статья 273 УК РФ - Создание, использование и распространение вредоносных компьютерных программ;
- Статья 274 УК РФ - Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-коммуникационных сетей;
- Статья 274.1 УК РФ - Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

### СОЦИАЛЬНЫЕ СЕТИ

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты.



**ЧТО ТАКОЕ СОЦИАЛЬНАЯ СЕТЬ?**

«Новый тренд» в Интернете, социальные сети, начались в 1995 году с американского портала Classmates.com («Одноклассники» является его русским аналогом). Проект оказался весьма успешным, что в следующие несколько лет спровоцировало появление десятка похожих сервисов. Но официальным началом бума социальных сетей принято считать 2003—2004 годы, когда были запущены LinkedIn, MySpace и Facebook. В Россию мода на социальные сети пришла двумя годами позже — в 2006-м, с появлением «Одноклассников» и «ВКонтакте».

Социальные сети стали своего рода Интернет-пристанищем, где каждый может найти базу для создания своего виртуального «Я». При этом каждый пользователь получил возможность не просто общаться и творить, но и делиться плодами своего творчества с многомиллионной аудиторией той или иной социальной сети.

Однако многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. Информацию об участниках социальных сетей могут найти их работодатели, бывшие или настоящие жены или мужья, сборщики долгов, преступники и так далее.

**РИСКИ В СОЦИАЛЬНОЙ СЕТИ**

Самый главный риск — это потеря персональных данных и информации для доступа к аккаунту. Потеря контроля за профайлом может привести к различным последствиям, таким как рассылка спама и зараженных файлов от вашего имени или опубликование вашей переписки с друзьями;

Информация, которая появляется в интернете в отношении вас, может очень повлиять на вас сейчас и в будущем. Например, вы можете показывать, что вы лентяй или можете быть очень вульгарным в общении в социальной сети, что характеризует вас с плохой стороны. Именно такой вывод сделает менеджер по персоналу, который будет принимать решение о приеме вас на работу.

Вы можете заинтересовать не только кибер, но и других преступников. Например, размещая информацию о своей квартире, благосостоянии вашей семьи, сообщая, куда

вы с семьей поедете на каникулы, вы можете заинтересовать воров;

Через социальные сети возможно заражение вашего компьютера. Злоумышленники могут взломать ваш профайл, и получить доступ к аккаунту.

**СОВЕТЫ ПО БЕЗОПАСНОСТИ**

Ограничьте список друзей. У вас в друзьях не должно быть случайных и незнакомых людей.

- Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату вашего рождения и другую личную информацию.
- Защищайте свою репутацию — держите ее в чистоте и задавайте себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить;
- Используйте настройки конфиденциальности аккаунта. Настройте просмотр содержимого вашей учетной записи «только для друзей»;
- Принимайте запросы в друзья только от тех людей, которых вы знаете и которым доверяете;
- Не используйте веб-камеру для общения с людьми, которых вы не знаете;
- Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место учебы и прочее;
- Если вы действительно хотите встретиться с человеком, с которым познакомились в интернете, то договоритесь о встрече в общественном месте, возьмите с собой друга. Если сетевой друг считает, что присутствие кого-то еще плохая идея, то стоит отказаться от встречи;
- Избегайте размещения фотографий в Интернете, где вы изображены местностью, по которой можно определить ваше местоположение;
- При регистрации в социальной сети необходимо использовать сложный пароль, состоящий из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу;
- Не размещайте фотографии и видео со своими друзьями без их разрешения. Обращайтесь к друзьям, чтобы они также соблюдали конфиденциальность и не размещали ваши фотографии и видео в общем доступе;
- Никогда не открывайте подозрительные ссылки, даже если они пришли от друзей. Удостоверьтесь в том, что друг выслал эту ссылку сам, а его аккаунт контролирует кибер-преступник.

