лига безопасного интернета

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ

БЕЗОПАСНЫЙ ИНТЕРНЕТ

Материалы к уроку безопасного Интернета

Москва, 2022

ЗАЧЕМ ЭТО ПОСОБИЕ?

Дорогие друзья! Перед Вами учебное пособие, разработанное экспертами Лиги безопасного Интернета. На страницах вы найдете практические советы как безопасно проводить время в сети.

Это пособие станет для вас навигатором по безопасному Интернету. Как сохранить свои персональные данные? Чем опасно общение с незнакомцами в сети? И почему цифровая зависимость – это не миф, а серьезная проблема? На эти и многие другие вопросы вы найдете ответы в учебнике, который находится в ваших руках!

Директор Лиги безопасного Интернета
Екатерина Мизулина

Интернет – это пространство не только возможностей, но и угроз. Конечно, вы уже знакомы с ресурсами цифрового мира и давно являетесь постоянными пользователями Интернет. Однако, эти прикладные знания должны опираться на «подушку безопасности» – культуру поведения в сети. Предлагаемые материалы, созданные «Лигой безопасного Интернета», могут стать основанием для интенсивной работы, ещё раз привлекут ваше внимание к проблемам агрессивной цифровой среды.

Разработчики предполагают наглядный материал для демонстрации на занятии или самостоятельной работы, памятки с конкретными советами, опираясь на ваш личный опыт, включение вас в актуальную дискуссию, в рамках которой вы сможете найти решение проблемных ситуаций, возникающих в сети. Конечно, по окончании изучения каждой темы вы должны применять полученные знания на практике, выполняя те или иные задания: например, «придумай себе надежный пароль».

Информация в памятках, таких как «Мошенничество в Интернете», может стать темой индивидуального образовательного проекта.

Авторский коллектив Лиги безопасного Интернета

СОДЕРЖАНИЕ

СКОЛЬКО ВРЕМЕНИ ТЫ ПРОВОДИШЬ В ИНТЕРНЕТЕ?

Знаешь ли ты, кто такой Билл Гейтс? Это один из создателей операционной сети Windows, которая, скорее всего, стоит и на твоем компьютере. Можно сказать, что именно этот человек создал для нас те компьютеры, которыми мы пользуемся. Как ты думаешь, сколько времени в день он разрешал своим детям проводить за компьютером?

Ответ тебя удивит: 45 минут в будни и 1 час, 45 минут в выходные. При этом он не разрешал детям пользоваться компьютером вечером перед сном, а до 14 лет и вовсе не давал им в руки гаджетов.

Другой известный человек, Стив Джобс, основатель Apple и создатель знаменитого «Айфона», запрещал своим детям пользоваться гаджетами по ночам и в выходные дни, а также во время еды.

Электронные развлечения легко вызывают самую настоящую зависимость. Будь внимателен и сам старайся следить за собой. Бей тревогу, если заметил у себя следующие признаки:

1. Не ложишься спать, предварительно не посидев в смартфоне.
2. Каждый день ешь за компьютером или со смартфоном в руке.
3. Почти все выходные проводишь в Интернете, никуда не выходя.
4. Злишься или раздражаешься, когда приходится отложить смартфон или оторваться от Интернета;
5. Не высыпаешься, часто испытываешь головные боли или неприятные ощущения в глазах.

Если ты хочешь избежать Интернет-зависимости, то старайся придерживаться следующих правил:

1. Сократи время использования гаджетов и компьютера.
2. Не бери в руки телефон хотя бы за час до того, как планируешь лечь спать. Интернет, соцсети или игры могут вызвать яркие эмоции, которые помешают уснуть.
3. Не ешь за компьютером и не используй телефон во время еды. Отвлекись от них ненадолго, лучше вместо этого пообщайся с родственниками или друзьями.
4. Старайся на выходных использовать компьютер и гаджеты как можно меньше. В Интернете или в играх очень легко «зависнуть» и весь день пролетит незамеченным, а ты потом будешь сожалеть о потерянном свободном времени.

Внимательно посмотри на свой телефон. Ты знаешь, что современные смартфоны – те же самые компьютеры? Они обладают такими же функциями, а в чем-то даже превосходят компьютер или ноутбук. **Наши телефоны включены круглосуточно. И все это время они собирают о нас информацию.**

Больше всех информацию собирают приложения соцсетей и мессенджеров. Фото, видео, история переписок, хобби и увлечения, даже места, в которых ты бываешь – все это приложения собирают и хранят. А все, что однажды попало в Интернет, остается там навсегда и удалить это невозможно.

Вся эта информация называется цифровым следом, который каждый из нас оставляет в сети. Невозможно пользоваться Интернетом и не оставлять след. Даже если ты решишь ничего не публиковать, ничего никому не писать, в любом случае прочитанные и просмотренные посты будут формировать длинную историю твоей активности. Этот след уникален для каждого человека, двух одинаковых быть не может. О каждом из нас в Интернете настолько много информации, что можно создать настоящего цифрового двойника.

В Интернете, как и в реальной жизни, нужно быть очень внимательным со своими словами и действиями. А из Интернета, как мы помним, ничего не удаляется. Всегда помни: чем меньше мы используем гаджеты – тем лучше!

Возможна ли анонимность в сети? Многим до сих пор не дает покоя этот вопрос, но на него есть однозначный ответ.

АНОНИМНОСТЬ В СЕТИ – МИФ!

Многим людям до сих пор кажется, что Интернет – безопасное и абсолютно анонимное место, где каждый может писать и делать все, что ему вздумается. Но это не так. Может быть когда-то Интернет таким и был, но сейчас следует помнить два важных правила:

1. Все, что однажды попало в Интернет, остается там навсегда.
2. В Интернете можно найти кого-угодно, даже если пользователь попытался скрыть о себе всю информацию.

Каждое твое действие в Интернете содержит информацию о том устройстве, с которого вы это делали – например, о телефоне или компьютере. А твой Интернет-провайдер видит все, что ты делаешь в Интернете несмотря на любую программу.

Важно помнить, что Интернет – это такое же публичное пространство, как улица, парк или школа. Там действуют те же правила – общайся прилично, соблюдай правила поведения и относись к другим людям так же, как хочешь, чтобы относились к тебе.

Ведь каждое действие или грубость в Интернете может иметь последствия. **Уважай других людей, относись с пониманием и состраданием к чужой беде.** Научись ставить себя на место другого человека. А также больше времени проводи в реальном мире, общаясь с друзьями по-настоящему, а не в сети.

Мистер Аноним

Washington, D.C., США

ЗАПОМНИ!

Анонимность в Интернете — это **миф!**

Следы пребывания в Интернете хранятся долго, даже прокси и анонимайзеры **не помогут скрыться!** Веди себя в Интернете вежливо, как в реальной жизни

ЗАДУМАЙСЯ, С КЕМ ТЫ ОБЩАЕШЬСЯ В ИНТЕРНЕТЕ, КТО СКРЫВАЕТСЯ ПОД НИКОМ?

Александр Ревва

ООО "САМЫЙ КРАСИВЫЙ"

Александр Ревва

Донецк, 44 года

не указан

Александр Ревва

ООО

Подтверждённая страница

Эта отметка означает, что страница Александра подтверждена администрацией ВКонтакте.

ВНИМАНИЕ: БУДЬ ОСТОРОЖЕН ПРИ ОБЩЕНИИ С НЕЗНАКОМЦАМИ В СЕТИ! ИМИ МОГУТ ОКАЗАТЬСЯ:

- **Маньяки, педофилы.** Завлекают в свои сети, делают неприличные предложения! Такое общение может быть опасным для жизни!
- **Интернет-ХАМЫ (Тролли)** провоцируют на необдуманные поступки и необоснованную агрессию!
- **Киберпреступники** зачастую обманом похищают чужое имущество!
- **Хакеры** используют анонимность для распространения вредоносного программного обеспечения, завладения учетными данными, платежными реквизитами, персональной информацией!

ТРАВЛЯ В ИНТЕРНЕТЕ

Травля в Интернете является большой проблемой для всех пользователей. Травлю в сети еще называют **кибербуллингом**.

Некоторым кажется, что травля – это всего лишь безобидные шутки. На самом деле это не так. Травля может привести к проблемам со здоровьем, к психическим травмам и другим проблемам. Иногда обижая других, обидчик стремится самоутвердиться за чужой счет.

ВИДЫ ТРАВЛИ

ОСКОРБЛЕНИЕ

Оскорбительные комментарии и вульгарные обращения в публичном пространстве Интернета.

КЛЕВЕТА

Выставление жертв в неблагоприятном свете с помощью фото- и видеоматериалов. Создание специально смонтированных фото или видео о жертве.

ПУБЛИЧНОЕ РАЗГЛАШЕНИЕ ЛИЧНОЙ ИНФОРМАЦИИ

Распространение личной информации для шантажа или оскорбления жертвы.

ДОМОГАТЕЛЬСТВО

Кибер-атаки от незнакомцев, адресованные конкретно Вам.

ПРЕСЛЕДОВАНИЕ И ПРОДОЛЖИТЕЛЬНОЕ ДОМОГАТЕЛЬСТВО

Продолжительное преследование жертвы, которое сопровождается домогательствами и угрозами

ИСПОЛЬЗОВАНИЕ ФИКТИВНОГО ИМЕНИ

Выдавать себя за другого человека, используя пароль жертвы

УГРОЗА ФИЗИЧЕСКОЙ РАСПРАВЫ

Угрозы причинения телесных повреждений и угрозы убийства

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТРАВЛИ, ВОСПОЛЬЗУЙТЕСЬ СЛЕДУЮЩИМИ ПРАВИЛАМИ:

КАК НЕ СТАТЬ ЖЕРТВОЙ ТРАВЛИ

1

Не вступайте в словесные перепалки в комментариях, на форумах, в беседах. У комментаторов может появиться желание мести.

2

Чаще **меняйте пароли** в соц. сетях, так как злоумышленники могут писать от Вашего имени.

3

Игнорируйте сообщения, в которых Вас оскорбляют или угрожают. Также стоит **уведомить** о таких сообщениях администрацию сайта или сервиса.

4

Не угрожайте хулигану «найти и наказать». Это лишь усугубит ситуацию.

5

Не выкладывайте в сеть лишнюю информацию или файлы, которые могут компрометировать Вас или Ваших знакомых. **Также не стоит** отправлять такую информацию людям, которые не вызывают доверия.

6

Не присоединяйтесь, если Ваши друзья дразнят кого-то в сети. Попросите их остановиться, предупредите о вредных последствиях травли.

7

Удалите злоумышленника из соцсетей, **заблокируйте** доступ к Вашей странице, **добавьте** в черный список.

8

Поговорите с родителями или учителями об этой ситуации. Они не оставят Вас одного в неприятном состоянии и помогут наилучшим способом разрешить любую ситуацию.

9

Вместе с родителями **соберите доказательства:** сделайте скриншоты переписки, скопируйте ссылки на аккаунты обидчика, Вам это может пригодиться в случае обращения в полицию.

Интернет – это возможность общаться с друзьями на расстоянии, не терять связь на летних каникулах и обсуждать интересные темы. Но также в Интернете есть много незнакомых пользователей, которые не просто так хотят добавить тебя в друзья и начать общение. Если ты не уверен в том, стоит ли добавлять того или иного пользователя в друзья, то лучше этого не делать. Незнакомцы в Интернете могут оказаться не теми, за кого себя выдают.

ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ:

1. Страницы в социальных сетях **лучше закрыть от посторонних**. Если ты не знаешь, как это сделать, то попроси родителей тебе помочь. Это защитит твои личные данные от попадания в руки преступников. Как правило, информацию о себе, своих увлечениях, хобби, фото с друзьями и многое другое мы публикуем в соцсетях. Очень часто информацию о нас злоумышленники берут в открытом доступе.

1. **Будь осторожен**, когда добавляешь незнакомого человека в друзья, особенно того, кого ты не знаешь в реальной жизни. Если же новый знакомый задает тебе много вопросов о семье или о том, где ты живешь и учишься, то никогда не рассказывай ему эту информацию. Сразу же сообщай о подозрительном незнакомце своим родителям.

1. **Будь внимателен**, если в переписке тебя призывают к действию и пытаются подловить. Об этом свидетельствуют такие фразы, как: «А ты сможешь или тебе слабо?» «Все мои знакомые уже это делали, в этом нет ничего такого» и аналогичные. Такие фразы должны тебя насторожить. Рекомендуем сразу блокировать подобные аккаунты.

1. **Не соглашайся на встречу с людьми из Интернета**. Под профилем твоего ровесника могут сидеть далеко не девочки и мальчики, а самые настоящие преступники. Всегда сообщай своим родителям о своих друзьях из Интернета, а также о том, куда ты направляешься, с кем собираешься встретиться во избежание опасности.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Персональные данные – это все ключевые и важные сведения о человеке. Их следует тщательно беречь и не раскрывать в Интернете без необходимости. Раскрытие персональных данных в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже аккаунтов, мошенническим действиям, краже денег и документов. В некоторых случаях это даже может привести преступника на порог твоего дома.

ЧТО ОТНОСИТСЯ К ПЕРСОНАЛЬНЫМ ДАННЫМ?

1. **Фамилия, имя, отчество;**
2. **Все твои документы** (паспорт, свидетельство о рождении, аттестат);
3. **Банковские данные** (номер счета, карты, пин-код, CVV-код);
4. **Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы);
5. **Фотографии и видеозаписи с твоим изображением;**
6. **Данные о твоих родственниках;**
7. **Твои логины и пароли.**

ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ЛИЧНАЯ ИНФОРМАЦИЯ В ИНТЕРНЕТЕ

Персональные данные — твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Персональные данные охраняет Федеральный Закон № 152 — ФЗ «О персональных данных»

КОМУ И ЗАЧЕМ НУЖНА ТВОЯ ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ?

- **80%** преступников берут информацию в соц. сетях
- Личная информация используется **для кражи паролей**
- Личная информация **используется для** совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение!

Кто может писать мне личные **сообщения**	Все пользователи
Кто видит **фотографии, на которых меня отметили**	Все пользователи
Кто видит **видеозаписи, на которых меня отметили**	Все пользователи
Кто может видеть список **моих аудиозаписей**	Все пользователи
Кого видно в списке **моих друзей и подписок**	Всех друзей
Кто может видеть моих с**крытых друзей**	Только я

При регистрации в соц. сетях следует использовать **только Имя или Псевдоним (ник)!**

Настрой **приватность** в соц. сетях и других сервисах

Не публикуй информацию о местонахождении и материальных ценностях!

Хорошо подумай, какую информацию можно публиковать в Интернете!

Не доверяй свои секреты незнакомцам из Интернета!

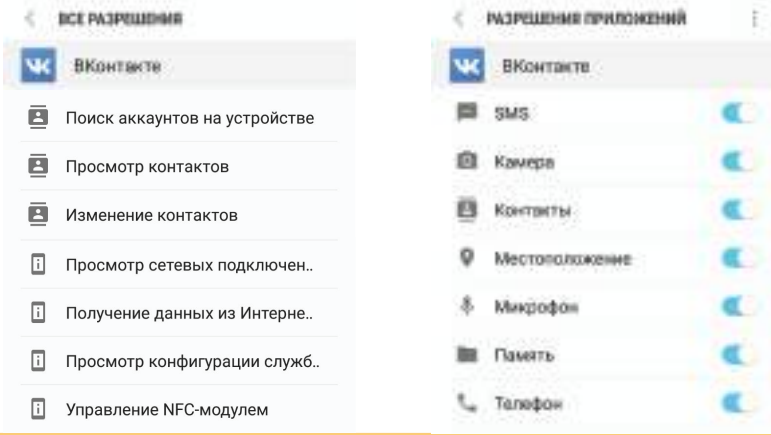
МОБИЛЬНЫЕ УСТРОЙСТВА/МОБИЛЬНЫЙ ИНТЕРНЕТ

Современный мобильный телефон/планшет — это не просто средство связи или красивая игрушка, а **полноценное коммуникационное устройство** не уступающее по производительности и функционалу персональному компьютеру

ВНИМАНИЕ! ПЕРСОНАЛЬНЫЕ ДАННЫЕ!

СЕГОДНЯ МОБИЛЬНЫЕ УСТРОЙСТВА СОДЕРЖАТ ВАЖНУЮ ИНФОРМАЦИЮ:

- Список **контактов**
- Личные **фотографии/видеозаписи**
- **Данные доступа** к электронной почте и иным аккаунтам в сети
- Данные о банковских **картах/платежах**
- Имеют привязку **к балансу** сим-карты оператора связи



- Установи **антивирус** на свое мобильное устройство
- Установи приложения из проверенных источников, **шифрующие** данные — они защитят личные файлы

- **Отключи** функцию автоподключения к открытым Wi-Fi сетям
- Используй только **защищенные Wi-Fi сети**
- Обязательно правильно **завершай работу** с публичным Wi-Fi

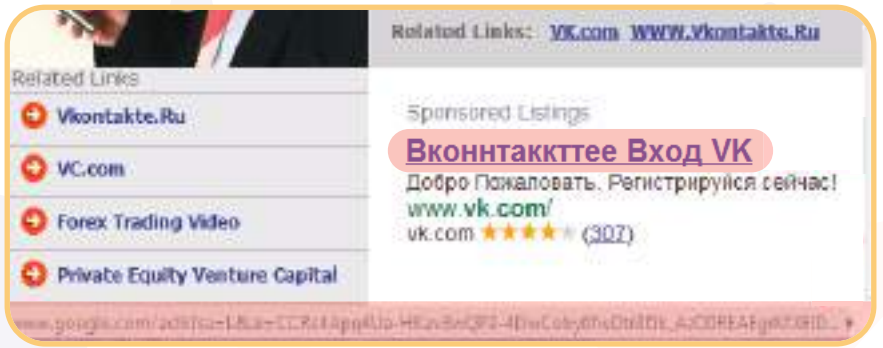
- Внимательно **изучай права,** запрашиваемые мобильными приложениями
- **Используй** только проверенные мобильные сервисы

ЧЕМ ОПАСНЫ САЙТЫ-ПОДДЕЛКИ?

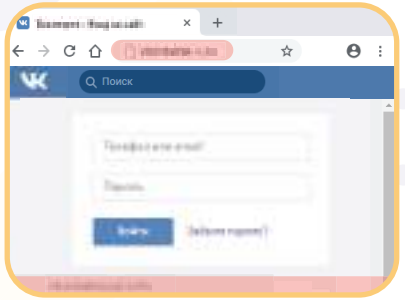
- Крадут пароли
- Распространяют вредоносное ПО
- Навязывают платные услуги
- Используют процессор компьютера для нелегального майнинга криптовалюты

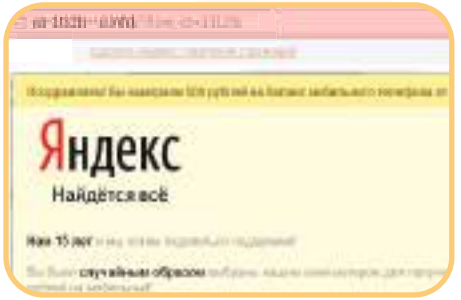
КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ? КАК ОПРЕДЕЛИТЬ ПОДДЕЛКУ? КАК ОБЕЗОПАСИТЬСЯ?

- Используй функционал браузера: **«избранное», «закладки»!**
- http **Проверяй** адрес сайта!
- Обрати внимание на **настоящий адрес** сайта!*
- Используйте **ad-blockers** (блокировщики рекламы)
- Большинство браузеров имеет **встроенные системы защиты,** предупреждающие, что сайт, на который вы собираетесь перейти, может быть не безопасен — **не игнорируйте** подобные предупреждения



*Адрес отображается во всплывающей подсказке





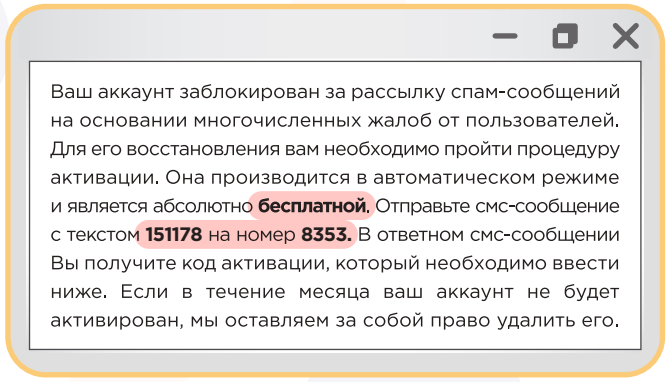
ОСТОРОЖНО, ПОДДЕЛКА!

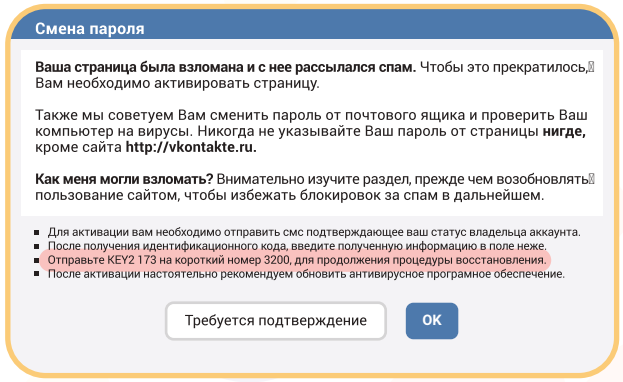
КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ?

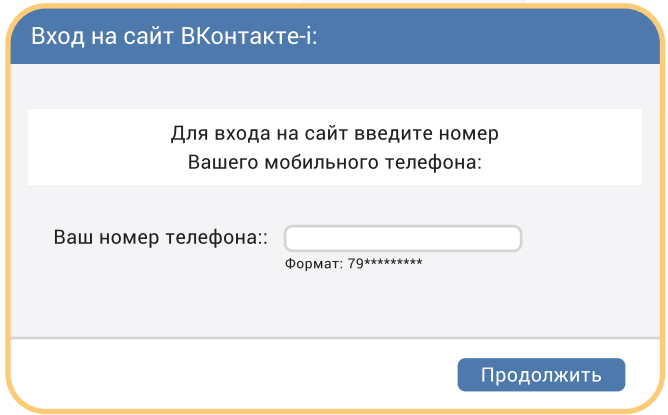
- Просят подтвердить логин/пароль
- Предлагают бесплатный антивирус, а устанавливают вредоносное ПО, вирусы
- Просят отправить СМС (платное)

КАК РАСПОЗНАТЬ ОБМАН? СОМНЕВАЕШЬСЯ?

- Закрой страницу, блокировка пропала? Все в порядке!
- Проверь систему антивирусом!
- Авторизуйся под своими аккаунтами и убедись, что все в порядке!
- Смени пароли аккаунтов, которые используешь!







Спам — это **массовая рассылка** незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания

Первоначально слово **«SPAM»** появилось в **1936 г.** Оно расшифровывалось как **SPiced hAM** (острая ветчина) и было товарным знаком для мясных консервов

ПОМНИ: ИДЯ НА ПОВОДУ У СПАМА ЕСТЬ РИСК:

- Отправить платное СМС, оплатить навязанную услугу
- Получить платную подписку на ненужную информацию
- Потерять учетные и (или) иные данные
- Стать жертвой обмана

БУДЬ ВНИМАТЕЛЕН!

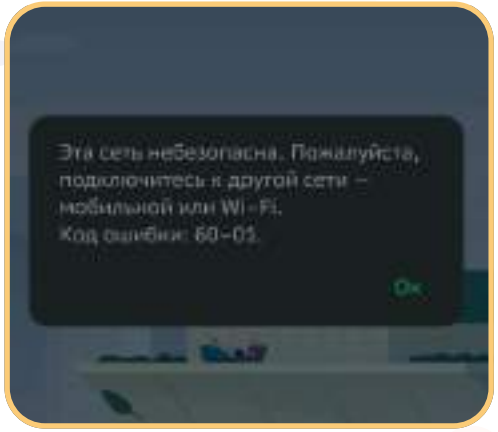
- **Настрой безопасность** браузера и почтовой программы (подключи антифишинг, защиту от спама и др. встроенные средства защиты)!
- Используй **дополнительные расширения** браузеров, например, блокировщики рекламы.
- Используй **Антивирус!**
- **Проверяй надежность** поставщика услуг!

ОТКРЫТЫЕ СЕТИ, ЧУЖАЯ ТЕХНИКА

НЕБРЕЖНОЕ ОТНОШЕНИЕ К ЛИЧНОЙ ИНФОРМАЦИИ МОЖЕТ ПРИВЕСТИ К ЕЕ УТЕРЕ!

ВСЕГДА ПОМНИ:

- **Будь осторожен** в открытых и небезопасных сетях. **Подключение к ложной сети** может моментально **лишить** тебя всей персональной информации, хранящейся в твоем электронном устройстве: преступнику **станут доступны** пароли и другая информация
- **Опасно оставлять** свои учетные данные на устройстве, которое тебе **не принадлежит,** этими данными могут воспользоваться в преступных целях



Несколько простых правил, которые следует соблюдать при работе в открытых сетях или с использованием «чужой» техники:

- При работе с публичным устройством используй пункт **«чужой компьютер»**
- Всегда используй режим **«приватного просмотра»** в браузере
- Всегда используй кнопку **«выйти»** при завершении работы с ресурсом
- **Отказывайся** от сохранения пароля при работе на «чужом компьютере»

- Используй только **безопасное соединение** с почтой и другими сервисами (безопасное соединение обозначено замком с зеленым текстом в адресной строке)
- Не оставляй **без присмотра** устройства доступа в сеть (телефон, планшет, ноутбук)

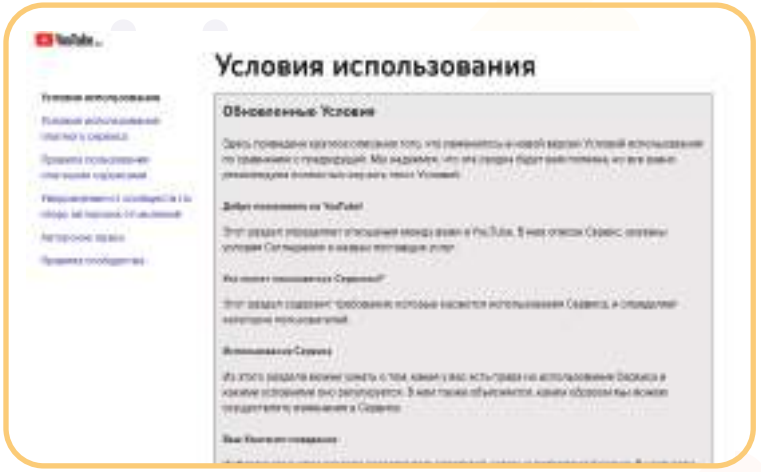
- Используй **шифрованные хранилища данных,** которые помогут **защитить** твои личные файлы
- Используй только **сложные пароли,** состоящие из прописных, заглавных латинских букв, цифр и символов
- Используй только **открытые сети,** в надежности которых ты **уверен**

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ПРОДУКТА

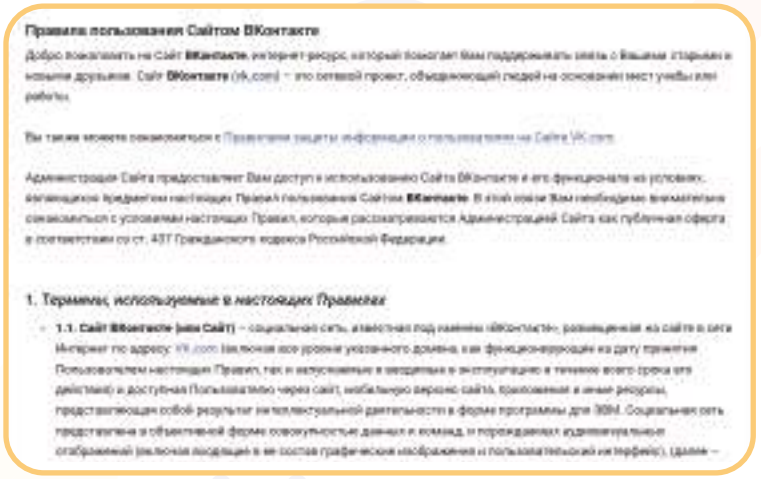
Любая услуга в Интернете имеет **лицензионное соглашения** и (или) **условия использования.** При установке программных продуктов (особенно от неизвестных производителей) следует **внимательно читать** тексты соглашений, ведь после принятия соглашения **вся ответственность и последствия** использования программного продукта **ложатся на тебя!**

ПОДТВЕРЖДАЯ СОГЛАШЕНИЕ «ВСЛЕПУЮ» ТЫ МОЖЕШЬ:

- **Оформить** платные подписки/услуги
- Предоставить приложению/программе **обширные права**
- **Лишиться** персональных данных, хранящихся на устройстве
- **Стать звеном** ботнета и (или) СПАМ сети
- **Стать жертвой** мошенников


Условия использования

Обновленные Условия


Правила пользования Сайтом ВКонтакте

1. Термины, используемые в настоящих Правилах

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ЗЛОУМЫШЛЕННИКОВ:

- Использовать лицензионные продукты **проверенного** производителя
- **Внимательно** знакомиться с лицензионным соглашением
- **Не использовать** подозрительное ПО

ПОМНИ: любые соглашения об использовании программных продуктов и услуг, даже от проверенного производителя, **требуют внимательного изучения!**

Помни: чем больше Всемирная Паутина проникает в жизнь людей, тем больше появляется злоумышленников, пытающихся всеми возможными путями лишить тебя денег!

КАРДИНГ И ФИШИНГ

Кардинг — способ мошенничества **с использованием банковских карт.** Преступники **похищают** реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя

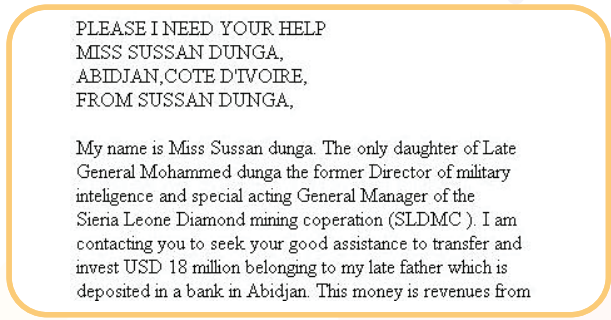
Фишинговые сообщения — это **уведомления,** отправленные **от имени администраторов** банковских или других платежных систем. Они призывают пользователей пройти по **фальшивой** ссылке, чтобы украсть конфиденциальные данные. Действия подобного рода нацелены на банковский счет или учетную запись в виртуальной платежной системе. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету

«НИГЕРИЙСКИЕ» ПИСЬМА, НЕВЕРОЯТНАЯ УДАЧА И ПОПРОШАЙКИ!

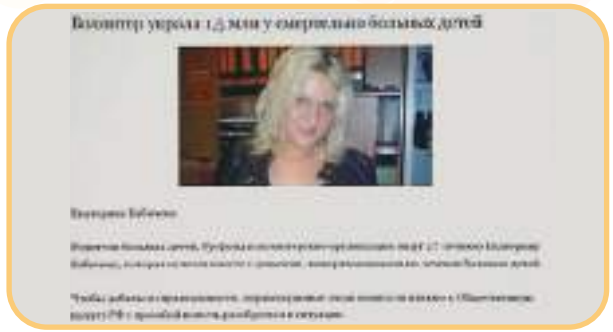
Уведомления о выигрыше: в письме сообщается о том, что ты выиграл крупную сумму денег. **Цель** мошенника — **выманить** у тебя **деньги** за получение выигрыша. Обычно он списывает это на налог. Потеряв бдительность, ты можешь перевести крупную сумму на счет мошенников

Попрошайничество: мошенники давят на жалость и отправляют **письма с просьбой о помощи** якобы от благотворительных организаций или нуждающихся людей. В действительности такие сообщения содержат ссылки на реальные организации и фонды, но реквизиты для перечисления денежных средств указываются ложные

«Нигерийские» письма: в тексте такого письма обычно содержится информация о том, что у автора письма **есть много денег,** полученных не совсем законным путем, и поэтому он не может хранить деньги на счету в банках своей страны. Ему срочно необходим счет за рубежом, куда можно перечислить деньги. Авторы подобных писем попросят тебя **обналичить** крупную денежную сумму, в качестве вознаграждения обещая **от 10% до 30%** от заявленной в письме суммы. Идея мошенничества заключается в том, что пользователь предоставит доступ к своему счету, с которого позже будут списаны все денежные средства


PLEASE I NEED YOUR HELP
MISS SUSSAN DUNGA,
ABIDJAN,COTE D'IVOIRE,
FROM SUSSAN DUNGA,

My name is Miss Sussan dunga. The only daughter of Late General Mohammed dunga the former Director of military inteligence and special acting General Manager of the Sieria Leone Diamond mining coperation (SLDMC). I am contacting you to seek your good assistance to transfer and invest USD 18 million belonging to my late father which is deposited in a bank in Abidjan. This money is revenues from



ЭЛЕКТРОННЫЕ ФИНАНСЫ

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ КРЕДИТНЫМИ КАРТАМИ В СЕТИ ИНТЕРНЕТ?

1

Всегда следует обращаться аккуратно со своими зарплатными, кредитными, дебитовыми картами, на которых есть доступные для списания средства. Для покупок через Интернет лучше **открыть отдельную карту,** на которую Вы будете переводить определенную сумму денег с основных карт.

2

Не упускайте из виду свою карту, когда передаете ее кассиру или официанту, ведь для того, чтобы совершить покупку в Интернете зачастую достаточно знать только номер карты и срок ее действия.

3

Следите за остатком на карте. Предпочтительно проверять баланс через специальную услугу SMS-информирования. Если Вы вовремя заметили транзакцию, которую Вы не совершали, ее зачастую можно отменить, подав соответствующую заявку.

4

Вводите номер карты и срок ее действия только на **проверенных сайтах,** желательно аккредитованных. Об этом Вам скажут логотипы платежных систем.

5

Популярные интернет-магазины предоставляют **специальные сервисы,** которые обеспечивают высокую безопасность банковских транзакций, а также сводят к минимуму возможности мошенников.

6

Многие компании-создатели антивирусных программ выпустили специальные пакеты для совершения **безопасных платежей** в сети Интернет.

6 ПРОСТЫХ ПРАВИЛ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

Если Вы решили проверить баланс своей кредитной карты онлайн, оплатить счета, перевести деньги кому-либо, купить или продать что-нибудь в интернете, то эти 6 простых правил помогут Вам не потерять деньги.

1

ЗАЩИТИ СВОЙ КОМПЬЮТЕР.

Своевременно проверяйте обновления ПО. Обязательно установите антивирусное ПО. Защитите свой wi-fi роутер паролем и используйте usb-накопители с осторожностью.

2

ТОЛЬКО СЛОЖНЫЕ ПАРОЛИ.

Самые эффективные пароли — написать русское словосочетание в английской раскладке клавиатуры. Пароль «Denis1986» взламывается просто, мы советуем Вам придумать **2 вида паролей:**

- длинные и сложные пароли для платежных систем;
- простые и легко запоминающееся для форумов и других, не представляющих опасности для ваших денег. Храните свои пароли в секрете. Не отправляйте их по SMS, e-mail или в соц. сетях.

3

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ. НАБИРАЙТЕ АДРЕС САЙТА САМОСТОЯТЕЛЬНО.

Переходя по ссылке из сомнительных источников (e-mail, форумы, сообщения в соц.сетях, всплывающие окна), Вы рискуете попасть на «фишинговый сайт» (фишинг — вид интернет-мошенничества, с целью получения доступа к конфиденциальным данным пользователей). При переходе на сайт обращайте внимание на адресную строку. Часто мошенники меняют одну или несколько букв в названии сайта (например: www.sberbank.ru/ — www.sbenbank.ru/).

6 ПРОСТЫХ ПРАВИЛ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

4

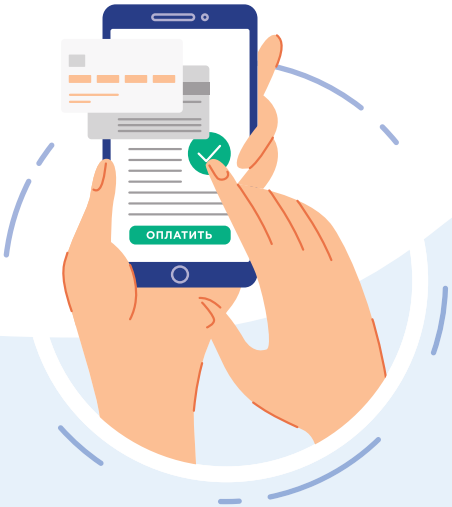
УСТАНОВЛЕНО ЛИ ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ?

В сети Интернет используется два протокола: HTTP и Secure HTTP. Прежде чем ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), обратите внимание на адресную строку, убедитесь, что имя протокола имеет вид **https://**, а не http (“s” — значит secure. англ. «защищенный»). Сертификаты подлинности получают только законопослушные компании, проверенные специалистами. Также о защищенности интернет-соединения свидетельствует значок амбарного замка на зеленом фоне рядом с адресной строкой.

5

ТРАНЗАКЦИИ ТОЛЬКО НА ДОМАШНЕМ КОМПЬЮТЕРЕ.

Никогда не проверяйте баланс личного счета, не оплачивайте счета, не совершайте покупки и другие операции с банковскими картами или электронными деньгами на компьютерах с общим доступом, а также на других мобильных устройствах (планшетах, телефонах), подключенных к публичным точкам доступа WiFi.



6

ПРИДЕРЖИВАЙТЕСЬ ЗДРАВОГО СМЫСЛА.

Чтобы защитить себя от мошенников, тщательно изучите эти простые советы. Внимательно относитесь к оповещениям из своего «банка». Часто злоумышленники присылают сообщения, в которых написано, что Ваш счет будет заблокирован, если Вы не предпримите немедленных действий, связанных с переводом денег, или представляются вашими родственниками или друзьями и требуют денег на операцию.

ОПАСНЫЕ СООБЩЕСТВА

В Интернете много опасных групп и сообществ, которые распространяют опасные для жизни и здоровья идеи, например, экстремальные и незаконные занятия, экстремистские или криминальные действия.

Обычно, аудитория таких сообществ отличается радикальными, а иногда и преступными убеждениями. Они готовы агрессивно навязывать свою позицию или даже причинять насилие.

В ЧЕМ ОПАСНОСТЬ ТАКИХ СООБЩЕСТВ?

- **Они могут быть опасны для твоего здоровья.** Некоторые занятия могут быть настолько опасны, что могут причинить твоему здоровью непоправимый вред.
- **Иногда это может даже привести к смерти!**
- **В таких сообществах тебя могут спровоцировать** или даже заставить (например, шантажом), причинить вред самому себе или другим людям, либо совершить что-либо незаконное.

Есть специальные люди, которые занимаются отбором пользователей в такие сообщества. Они называются «вербовщиками». Есть яркие признаки того, что тебя вербуют:

- **Собеседник** в Интернете пытается завладеть буквально всем твоим вниманием и временем. Он **очень навязчив.**
- **Тебя приглашают в какое-либо сообщество** с очень узкими интересами (не обязательно закрытое).
- **Тебе и другим пользователям в сообществе регулярно дают какие-либо задачи.** От простого «сделай репост публикации» до челленджей или «выйди на улицу и нарисуй граффити». Лучше не выполнять никаких задач, которые ставят в сообществах. Этим владельцы группы дрессируют пользователей в своих целях.

Доверяй своим родителям. В случае, если кто-то попытается втянуть тебя в сомнительную деятельность, в первую очередь обращайся именно к ним!

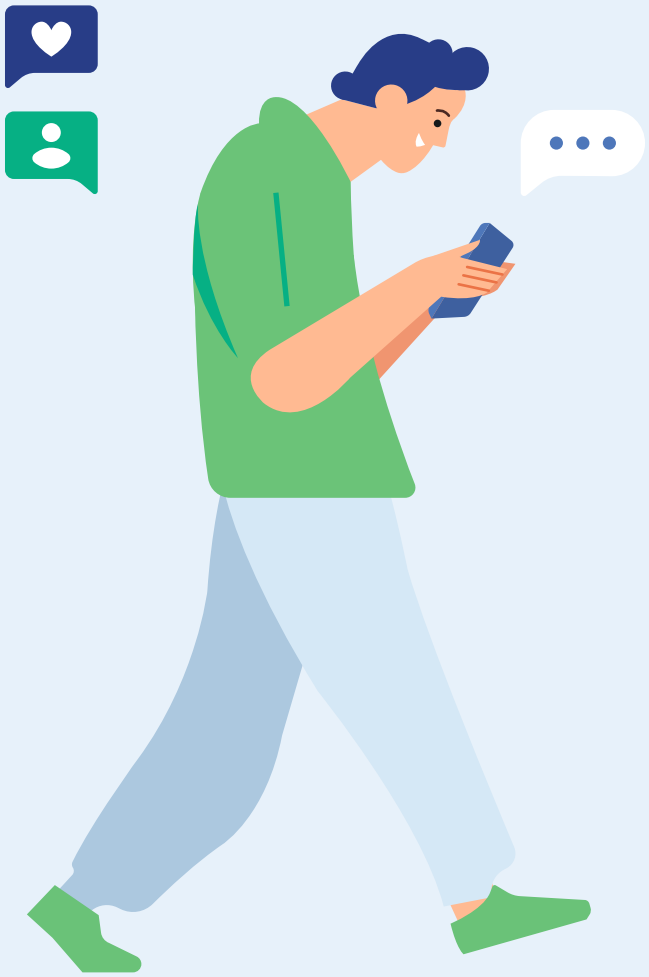
Возможно ты уже неоднократно сталкивался в Интернете с опасным контентом. Такой контент может, например, пропагандировать наркотики, экстремизм, насилие, ненависть по отношению к разным людям, содержать жестокие изображения или видео.

ЧТО ДЕЛАТЬ, ЕСЛИ ТЫ СТОЛКНУЛСЯ С ТАКИМ КОНТЕНТОМ?

- **Обратись к родителям.** Они подскажут тебе, что с этим можно сделать;
- **В социальной сети нажми «Пожаловаться»** и отправь жалобу администрации соцсети;
- **Если такой контент тебе прислали в соцсети или мессенджере – заблокируй отправителя,** а также нажми «Пожаловаться» в его аккаунте.

СОЦИАЛЬНЫЕ СЕТИ

СОЦИАЛЬНЫЕ СЕТИ



Социальные сети сегодня стали для нас **больше, чем просто среда общения** и обмена фотографиями. Простота работы со своими страничками со смартфонов и планшетов, недорогие тарифы для подключения мобильного интернета и доступный wi-fi позволяют быть on-line всегда и везде, а социальные сети превращаются **в устойчивую привычку**, без которой мы уже не можем представить современную жизнь.

Но легкая доступность сетей создает **новые возможности и новые угрозы** как для активных пользователей, так и для тех, кто проверяет свои «странички» один раз в день или реже.

Социальных сетей и социальных медиа с каждым днем **становится все больше** и все труднее выбрать какую-то одну для удовлетворения всех медийных потребностей. Но **разбираться в них необходимо**, чтобы избежать лишних трудностей и нежелательных последствий.

КАК ОТЛИЧИТЬ «ЛИПУ» ОТ ОРИГИНАЛА

КАК ОТЛИЧИТЬ СТРАНИЦЫ

В контексте соцсетей «липовыми» страницами называют поддельные страницы реальных людей с идентичными фотографиями и данными. **Как же отличить «липу» от оригинала?** Существует несколько признаков «липовых» страниц.

1

Фотографии, «вырванные» из других соц. сетей или поисковых сервисов. Когда Вы выкладываете фотографию, многие соц. сети помечают ее своим логотипом и скачать ее из сервиса без него невозможно. При скачивании таких фото теряется качество. Если Вы заметили, что в профайле «вконтакте» много фотографий из «одноклассников» и качество оставляет желать лучшего, вполне вероятно, что страница липовая.

2

«Пустой» профайл. Обычно создатели липовых страниц не особо стараются повторить оригинал: не указывают личную информацию, интересы и так далее. Если никаких данных, кроме имени, не указано, стоит насторожиться.

3

В общении с другими людьми обладатель липовой страницы обычно пишет общими фразами, никогда не указывает детали.

4

Если страница создана пару дней назад, а все фотографии загружены одной датой — это тоже, вероятнее всего, липа.

5

От липовых страниц приходит много спама, так как многие мошенники создают такие страницы для накрутки голосов или приглашения людей в свои ресурсы.

6

Первые 100 друзей у липовой страницы обычно реальные люди, поэтому, если вы решили проверить липовая страница или нет, просмотрите всех друзей в ленте.

7

Если указана школа/университет и год окончания, проверьте, есть ли в друзьях у человека люди из этой школы. Напишите им, спросите, знакомы ли они с человеком лично.

8

Посмотрите записи на стене и найдите первую. Когда она была сделана? Чем старше аккаунт, тем выше вероятность, что он реальный.

КАК ОТЛИЧИТЬ СТРАНИЦЫ

Страничка в соц. сетях — это **мощный инструмент** формирования имиджа человека, поэтому так необходимо **внимательно относиться** к тому, как она выглядит. Но **как найти эту грань** между излишней скрытностью и чрезмерным хвастовством?

Медиамир стал настолько реальным, что мы **воспринимаем страницу человека, как его самого.**

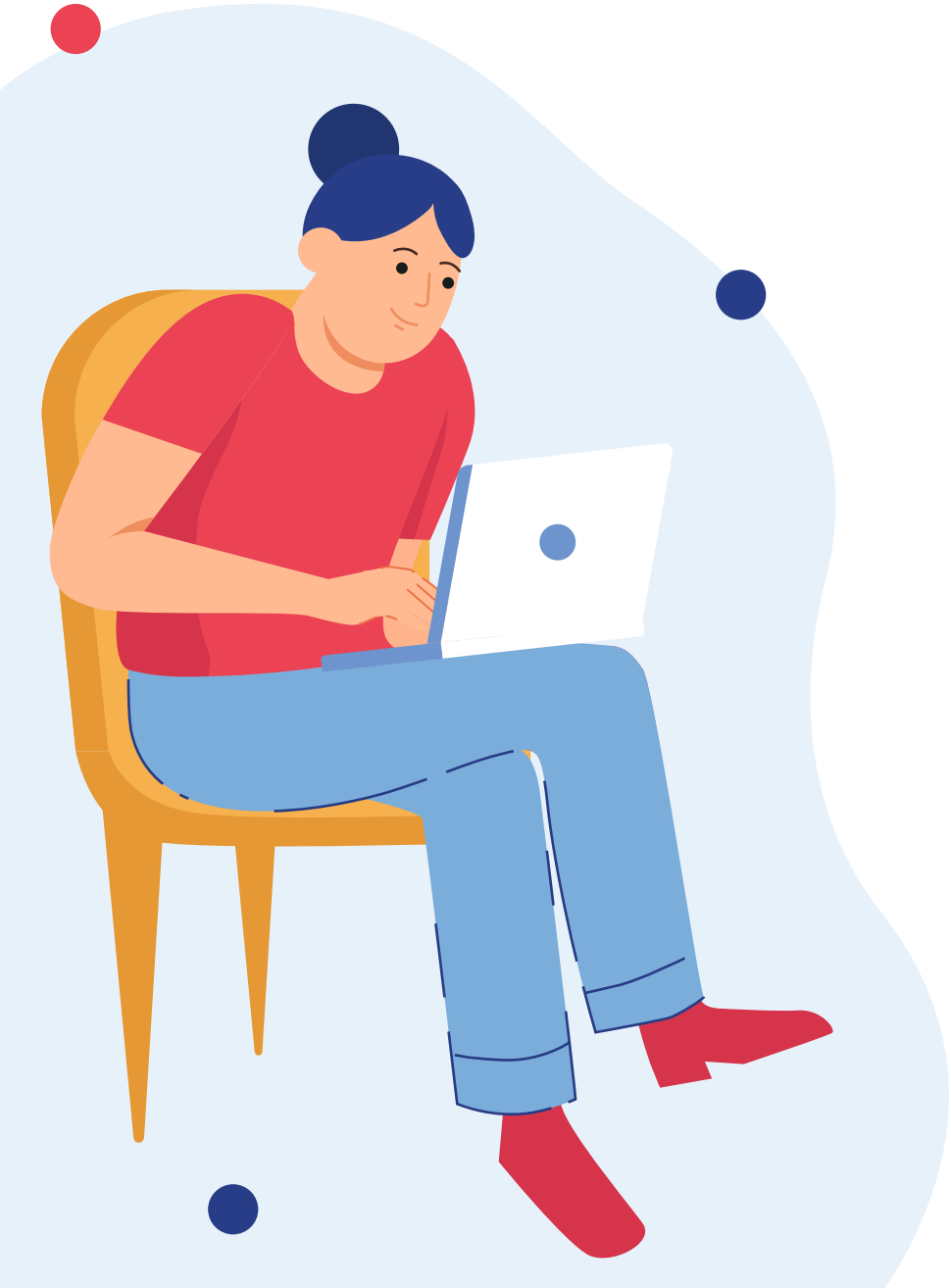
Если у Вас **«открытые»** аккаунты в соц. сетях, то нужно понимать, что информацию в них **может увидеть любой** пользователь. Важной проблемой становится **эмоциональная зависимость** от соц. сетей и излишняя **откровенность.** Контент страницы позволяет узнать Ваше окружение, интересы и виды активности.

Мы не призываем Вас оставлять аккаунты пустыми, но не стоит забывать о **настройках приватности.**

Нельзя забывать, что в современном мире **соц. сети** — это **ваше лицо.** И если Вы хотите произвести хорошее впечатление, оставляйте все самое личное **«под замком».**

НЕ СТАРАЙТЕСЬ ПОКАЗАТЬСЯ В СЕТИ ЛУЧШЕ, ЧЕМ ВЫ ЕСТЬ

СОЗДАЕМ СВОЮ «СТРАНИЧКУ»



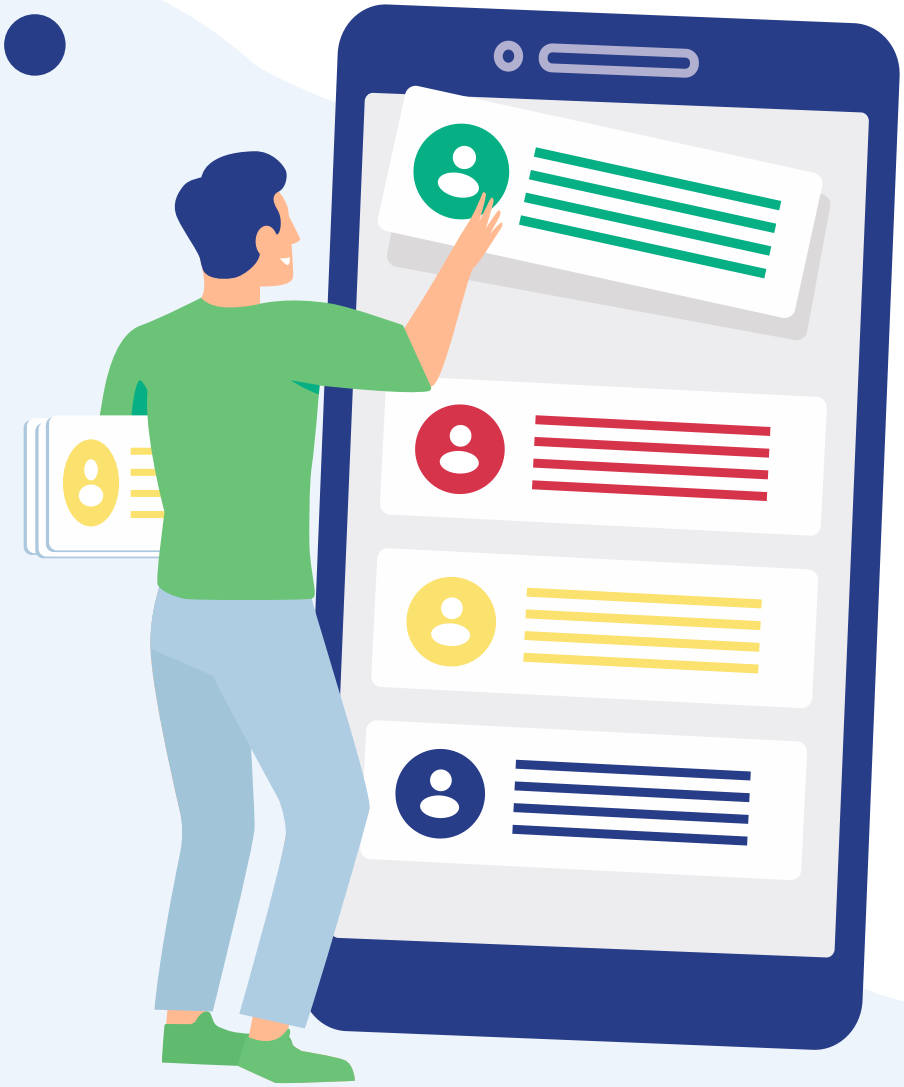
Для **регистрации** в любой социальной сети, Вам понадобится **адрес электронной почты**. Указывайте существующий email, так как с помощью него Вам нужно будет подтвердить Вашу личность. Обычно администрация сайта присылает письмо для подтверждения регистрации.

Помимо электронной почты для регистрации нужно **придумать логин,** который будет являться Вашим именем в сервисе.

Главная часть регистрации — это пароль. **Пароль не должен быть слишком простым,** иначе его будет легко подобрать, и тогда персональные **данные могут попасть в руки злоумышленников.** Не указывайте в качестве пароля дату своего рождения, используйте помимо цифр буквы с разным регистром.

После регистрации Вам будет предложено заполнить профиль: указать краткую информацию о себе, дату рождения, интересы, место работы/учебы и так далее. Также вы можете загрузить фотографию профиля — аватар. **Не стоит указывать личные данные и размещать фотографии, которые в дальнейшем могут Вас скомпрометировать.**

ОСНОВНЫЕ ПРАВИЛА ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ



Не нужно указывать **слишком много информации.** Помните, что другие пользователи, которые Вами заинтересуются, прочитают все до последней буквы.

Не следует выкладывать **фотографии или другие медиафайлы,** на которых Ваши друзья показаны **не в очень выгодном свете:** Вы можете испортить репутацию не только себе, но и знакомым.

Не используйте одинаковые пароли для разных сервисов. Этим могут воспользоваться злоумышленники.

Старайтесь писать сообщения **без использования жаргонной и ненормативной лексики,** с соблюдением правил орфографии и пунктуации. Общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, начальством или администрацией — это не допускается.

ВЕЧНАЯ ПУБЛИЧНОСТЬ В СОЦСЕТЯХ

Социальные сети давно стали частью нашей жизни. Виртуальное общение и развлечения стали неотъемлемой частью каждого дня.

Но, как ты помнишь, виртуальная жизнь вызывает зависимость. Для некоторых людей она целиком заменяет досуг или общение. Иногда люди, которые слишком много времени проводят в сети, пытаются поступать в реальной жизни так же, как они бы поступали в Интернете.

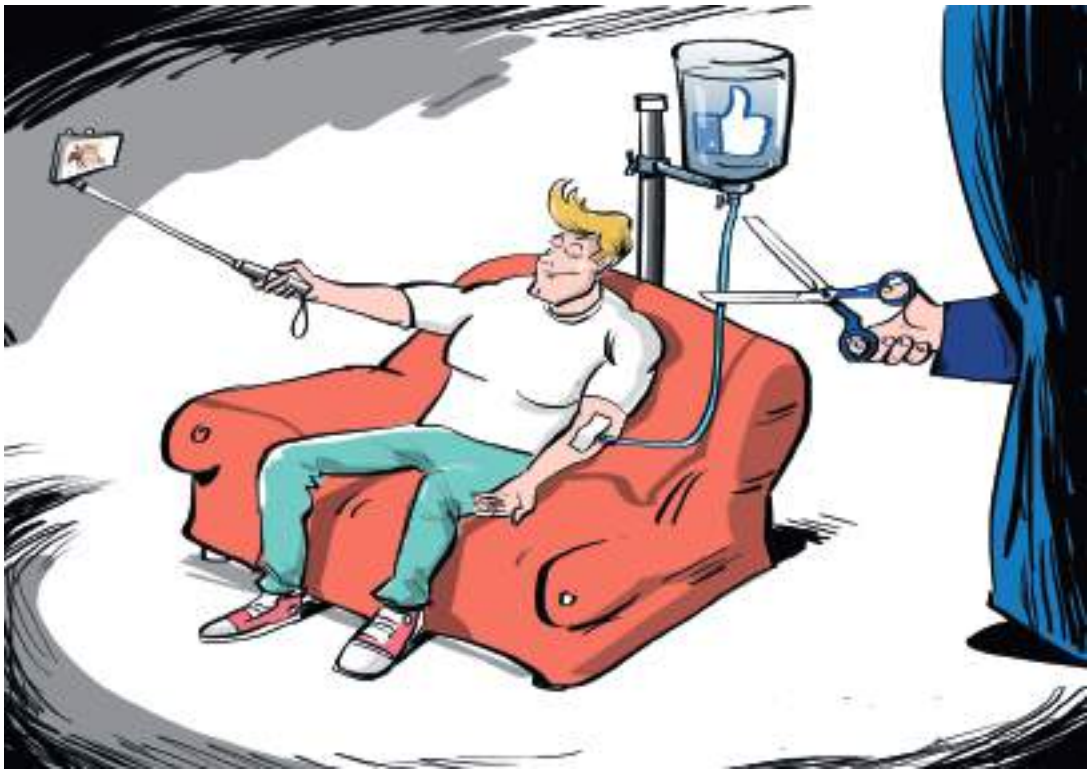
Обрати внимание, нет ли у тебя этих признаков:

- Во время неудобного разговора или спора вместо решения конфликта пытаешься уйти от разговора, перестать отвечать, игнорируешь собеседника. В соцсетях такое бы сработало, но в реальной жизни нельзя просто «забанить» собеседника.
- Писать на телефоне или на клавиатуре для тебя удобнее, чем ручкой на бумаге.
- Стараешься сфотографировать и опубликовать все происходящее с тобой. Еду, достопримечательности и т.д. Публикация в соцсети интересует тебя больше, чем само событие.

Социальные сети навязывают пользователям свои иллюзии. Некоторые люди, которые тратят в соцсетях все свободное время, начинают верить в эти иллюзии.

Иллюзия недолговечности – большинство пользователей уверено, что все, что они выложили в сеть, будет жить всего лишь несколько часов или дней. Это объясняется тем, что в соцсетях чем старше публикация, тем меньше людей ее видят, так как в ленте они воспринимают только наиболее свежие и актуальные публикации. Однако это не так! Старые публикации никуда не пропадают даже в случае их удаления пользователем. Они хранятся и формируют обширный цифровой след об авторе, а при необходимости могут быть восстановлены и использованы для шантажа или компромата.

Иллюзия доброжелательности – авторы публикаций в социальных сетях ожидают видеть преимущественно положительную реакцию, похвалу и одобрение в свой адрес. Несогласных или возмущенных людей можно просто «забанить», так они не смогут комментировать и даже просматривать публикации пользователя. Чем больше пользователь находится в плену этой иллюзии, тем меньше он готов к нападениям недоброжелателей и «троллей» в соцсети и тем сильнее будет травмирован в случае травли или агрессии.



Иллюзия ценности – многие пользователи уверены, что все, что они пишут и публикуют – нужно и полезно для остальных пользователей. В какой-то степени, это действительно так. Только вся эта информация нужна и полезна не для других пользователей, а для самой соцсети и ее разработчиков. Ведь чем больше информации о себе вы опубликуете, тем более точный портрет смогут собрать о вас алгоритмы соцсетей и тем более дорогую рекламу смогут вам показывать.

ВНИМАТЕЛЬНО СЛЕДИ ЗА ТЕМ, ЧТО И КОМУ ТЫ ОТПРАВЛЯЕШЬ В ИНТЕРНЕТЕ!

Излишне доверительное общение с незнакомцами в Интернете и рассылка своих фотографий или видео может привести к очень неприятным последствиям:

- **Травля** – фотографии и видео могут использовать тролли или агрессоры с целью травли, унижения и высмеивания.
- **Шантаж** – фото и видео могут использовать для шантажа и вымогательства денег.

Незнакомец в Интернете может представиться кем угодно. Например, твой ровесник, с которым ты познакомился в соцсети, может оказаться преступником, мошенником или даже маньяком.

Помни, что непристойные сообщения или просьбы в соцсетях необходимо блокировать, направляя жалобу в администрацию сайта.

Закрой свою страницу в соцсетях для посторонних и ограничь круг общения только теми людьми, которых ты знаешь в реальной жизни.

Что делать, если кто-то в Интернете написал тебе непристойное сообщение или обманом заставил тебя прислать свои фото и видео:

- В первую очередь обратись к родителям. Они подскажут, что нужно сделать дальше.
- Вместе с родителями напиши заявление в полицию.
- Сохрани скриншоты переписок. Это пригодится для доказательства преступления.

Фейки – это специально созданные ложные новости, которые распространяются с целью запутать людей, напугать их, посеять панику или дезинформировать.

Как не попасться на фейк:

- **Не верь всему, что пишут в Интернете!** Помни, что посты в соцсетях, статьи в некоторых энциклопедиях, даже новости на некоторых сайтах могут писать и редактировать любые люди. Некоторые делают это для шутки, а некоторые делают это специально, чтобы запутать других.
- **Помни, что любую информацию нужно перепроверять.** Если сомневаешься – обязательно спроси об этом у взрослых, родителей, посмотри на других сайтах.
- **Запомни навсегда**, что Интернет и соцсети – плохой источник новостей! **90% всего, что написано в Интернете – ложь.**

ПРОВЕРКА ФАКТОВ И ПОИСК ИСТИНЫ

В случаях, когда новость вызывает сомнения и ее необходимо проверить, следуйте следующим правилам:

1

Необходимо обратить внимание на **источник информации,** поскольку одним из доказательств достоверности является наличие ссылок на источники.

2

Свидетельства очевидцев — один из самых сложных методов проверки достоверности. Обратите внимание, подтверждает ли очевидец тезисы, о которых нам сообщает журналист.

3

Если в качестве доказательства достоверности Вам **предоставляют фото,** необходимо убедиться, что изображение действительно имеет отношение к описанным событиям. Для этого мы рекомендуем найти данную новость на каком-либо Интернет-ресурсе и воспользоваться сервисом Google или Яндекс «поиск по картинкам», далее следует обратить внимание на первоисточник и дату публикации, соотнести с источником информации.

4

Если Вы хотите проверить **подлинность видео,** перейдите на сайт YouTube, кликнув по логотипу в нижнем правом углу плеера, прочтите описание к видео, посмотрите, когда и кем данное видео было загружено, а также обратите внимание на комментарии к нему. Обращайте внимание на детали: номера машин, названия улиц.

МЕТОДЫ ОЦЕНКИ ИСТОЧНИКОВ ИНФОРМАЦИИ

1

Необходимо **убедиться в компетентности** источника, разбирается ли он в данном вопросе.

2

Если информация получена из Интернета, проверьте **регистрацию** ресурса как СМИ, иначе он имеет полное право публиковать любые «новости».

3

Также можно выяснить рейтинг источника, на котором размещена информация, его популярность, степень доверия и авторитетность.

НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ

Ученые выяснили, что прием поливитаминов может привести к возникновению рака.

«Группа американских и британских ученых провела ряд исследований и пришла к выводу, что прием поливитаминов может спровоцировать онкологические заболевания.»

Упоминания ученых должны стать сигналом о том, что автор материала либо не знает, либо скрывает имена конкретных людей, лабораторий и университетов. Таким сообщениям нельзя доверять, так как под прикрытием «ученых» можно рассказывать абсолютно любые небылицы и запутывать неопытных читателей.

«На протяжении длительного времени они изучали анамнез и истории болезни пятисот тысяч человек. Выяснилось, что побочным эффектом употребления поливитаминов может стать рак. Но это касается людей, которые придерживаются нормального пищевого рациона и одновременно принимают поливитамины.»

Если автор ссылается на исследования, то обязательно необходимо указывать название исследовательского проекта, группу исследователей, название организации. А также год и город. В противном случае, такая информация должна восприниматься не иначе, как авторский вымысел.

«Подобное заключение ученых вызвало ряд критики и неодобрения у скептиков. Последние уверены, что кроме правильного питания, в рацион людей необходимо добавить поливитамины. Что диета и правильный рацион не может обеспечить организм человека достаточным количеством витаминов.»

Здесь было бы уместно указать фамилии и должности «скептиков», у которых заключение ученых вызвало «ряд критики и неодобрения».

«Но множество других научных исследований подтверждают, что употребление поливитаминов не только не оправдывает возложенных на них надежд, а часто даже усугубляет болезни и провоцирует новые.»

Внешне логичная конва рассуждения смотрится как полноценное аналитическое сообщение, однако, если всмотреться внимательно в суть слов-якорей, окажется, что они совсем не имеют веса.

НОВОСТИ, КОТОРЫМ НЕЛЬЗЯ ДОВЕРЯТЬ

«С треском провалились исследования по изучению влияния, которое оказывает применение поливитамина Е на увеличение продолжительности жизни, снижение риска заболевания атеросклерозом. Продолжительность жизни людей, которые регулярно принимали витамин Е, оказалась на четыре процента ниже, чем у не принимавших. А вот прием витамина А и вовсе на шестнадцать процентов укоротил жизнь пациентов.»

Автор нанизывает, словно бусины, новые и новые факты, ссылаясь на исследования, имеющие громкий резонанс в научном сообществе, но вот совсем не понятно, что же это за исследование.

«Неожиданным стал результат эксперимента, целью которого стало исследование дополнительного приема пациентами поливитамина С. Оказывается, всеми любимая с детства аскорбинка влияет на развитие болезней сердца. Однако наблюдения за людьми, употребляющими в питании много овощей и фруктов, содержащих ту же аскорбиновую кислоту, но в натуральном виде, дали замечательные результаты — такие люди значительно реже заболевали раком и сердечно-сосудистыми болезнями.»

Динамика текста, противопоставление и сталкивание позиций создают ощущение привлекательности, и текст хочется дочитать до конца.

«Вывод напрашивается сам собой. Витамины полезны, но только в натуральном виде.»

Подобные тексты несут огромную опасность для читателей. Не потому, что можно перестать употреблять поливитамины, а потому, что таким же образом можно рассказать о кандидате на выборную должность, политическом и экономическом скандале, разжечь межнациональный конфликт.

КАК ВИРТУАЛЬНАЯ СЕТЬ МОЖЕТ ВЛИЯТЬ НА РЕАЛЬНУЮ ЖИЗНЬ

ПОМНИ: за **ВИРТУАЛЬНЫЕ** преступления отвечают по **РЕАЛЬНОМУ** закону

СТ. 272 УК РФ — Неправомерный доступ к компьютерной информации (**до 5 лет** лишения свободы)

СТ. 273 УК РФ — Создание, использование и распространение вредоносных программ для ЭВМ (**5 лет** лишения свободы)

СТ. 274 УК РФ — Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (**до 5 лет** лишения свободы)

СТ. 128.1 УК РФ — Клевета (**до 5 лет** лишения свободы)

СТ. 5.61 КоАП — Оскорбление (**штраф до 5000 рублей**)

СТ. 159 — Мошенничество (**до 10 лет** лишения свободы)

СТ. 165 — Причинение имущественного ущерба путем обмана или злоупотребления доверием (**до 5 лет** лишения свободы)

СТ. 146 — Нарушение авторских и смежных прав (**до 6 лет** лишения свободы)

СТ. 242 — Незаконное распространение порнографических материалов или предметов (**до 6 лет** лишения свободы)

СТ. 242 (1) — Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (**до 10 лет** лишения свободы)

Сейчас в каждую соцсеть и в мессенджеры можно загрузить видео или провести прямую трансляцию. **Видео и трансляции – отличный способ поделиться с друзьями своим творчеством.** Но нужно помнить, что твои видео увидят не только друзья!

ЧЕМ ЖЕ ОПАСНЫ ВИДЕО И ПРЯМЫЕ ТРАНСЛЯЦИИ?

- **Из любого видео,** в том числе из трансляции, **можно сделать скриншот** или записать видео, используя программы для захвата экрана. **Злоумышленники могут использовать эти кадры для травли или шантажа.**
- **На многих сайтах** обмена видео **нет возможности ограничить круг лиц,** которые могут смотреть видео.
- **На видео,** особенно в онлайн-трансляциях, **можно случайно выдать свои персональные данные.** Даже если ты не назовешь своего имени, зрители могут узнать, где ты живешь.
- **Комментарии** под видео, особенно под трансляциями, **не всегда можно проверять**. Они могут быть оскорбительного содержания, спровоцировать травлю или агрессию.

КАК ОБЕЗОПАСИТЬ СЕБЯ?

- **Тщательно ознакомься с сайтом**, приложением или сервисом, на котором планируешь выкладывать видео или вести трансляцию. Проверь настройки приватности, узнай, как можно подать жалобу на неприемлемый контент или комментарии.
- **Настрой параметры конфиденциальности** – сделай учетную запись закрытой. Хорошо, если на сайте есть возможность самостоятельно одобрять или отклонять подписчиков.
- **Ограничь число подписчиков** теми, кого знаешь в реальной жизни.

Даже в онлайн-играх может поджидать опасность. Многие игры имеют функцию чата. А это значит, что тебе может написать кто угодно и когда угодно. Незнакомец может прислать тебе опасный материал или ссылку, ведущую на опасный контент.

КАК ОБЕЗОПАСИТЬ СЕБЯ В ОНЛАЙН-ИГРАХ?

- Узнай, есть ли в игре функция чата? Если есть, можно ли ее отключить.
- Узнай, есть ли в игре модерация? Могут ли модераторы или администраторы следить за соблюдением правил, вежливым общением и контентом, которым обмениваются игроки?
- Ознакомься с правилами игры. Ты должен иметь возможность пожаловаться на другого игрока, если тот ведет себя неприлично, неуместно или совершает оскорбительные действия.

10 СОВЕТОВ ПО БЕЗОПАСНОСТИ

1. **Сокращай время пользования Интернетом!** Для общения с друзьями и развлечения нужно не так много времени. Вовсе не обязательно торчать в соцсетях весь день.

2. **Не забывай сам себя контролировать.** Помни, что у детей Стива Джобса вообще не было доступа в Интернет.

3. **Проводи больше времени в реальной жизни.** Общайся с друзьями, родителями, читай, занимайся спортом и хобби.

4. **Будь бдителен!** В Интернете много мошенников и преступников, которые охотятся за твоими деньгами или данными.

5. **Не выкладывай свои персональные данные в Интернет.** Помни, что отправлять их не стоит даже друзьям.

6. **Закрой свои страницы в соцсетях от посторонних.** Будь осторожен с незнакомцами в Интернете, а если кто-то из них задает тебе странные вопросы, навязывает общение или ведет себя агрессивно – блокируй такого человека и прекрати общение.

7. **Не бойся рассказать родителям о своих проблемах.** Если кто-то решит тебя обижать, травить, угрожать тебе, даже если ты попадешься на удочку мошенников, родители смогут помочь тебе и подскажут, как надо поступить.

8. **Помни, что из Интернета ничего не удаляется.** Если ты не хочешь, чтобы твои фото или посты увидели все друзья и знакомые – лучше вообще их не выкладывай.

9. **Не верь всему, что написано в Интернете.** В сети много вранья, многие заголовки пишутся просто для того, чтобы привлечь внимание. Если есть сомнения по поводу новости – лучше проверь, скорее всего это фейк.

10. **Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни.** Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

ЗАПОМНИ ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

Не уверен в своих знаниях? **Используй** учетную запись с ограниченными правами!

Не выкладывай свои персональные данные в Интернет! Помни, что их не стоит отправлять даже друзьям!

Закрой свои страницы в соцсетях от посторонних!

Используй **антивирус.** Коммерческие программы предоставляют дополнительные функции и удобства

Учитывай рекомендации программ защиты (не заходи на сайты, которые помечены как опасные, не открывай файлы, которые блокирует антивирус)

Настрой доп. функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска)

Помни, что из Интернета ничего не удаляется!

Не бойся рассказать родителям о своих проблемах. Родители смогут помочь тебе и подскажут, как поступить

Ограничивай время работы в Интернете — живи реальной жизнью!

ПОДРОБНЕЕ О ПРАВИЛАХ ЧИТАЙ НА САЙТЕ ЛИГИ БЕЗОПАСНОГО ИНТЕРНЕТА

www.ligainternet.ru

ВОПРОСЫ ДЛЯ ОБСУЖДЕНИЯ

Чем опасны сайты подделки?
Как распознать подделку?

Что такое Спам?
Как бороться со Спамом?
Какие существуют методы блокировки Спам рекламы?

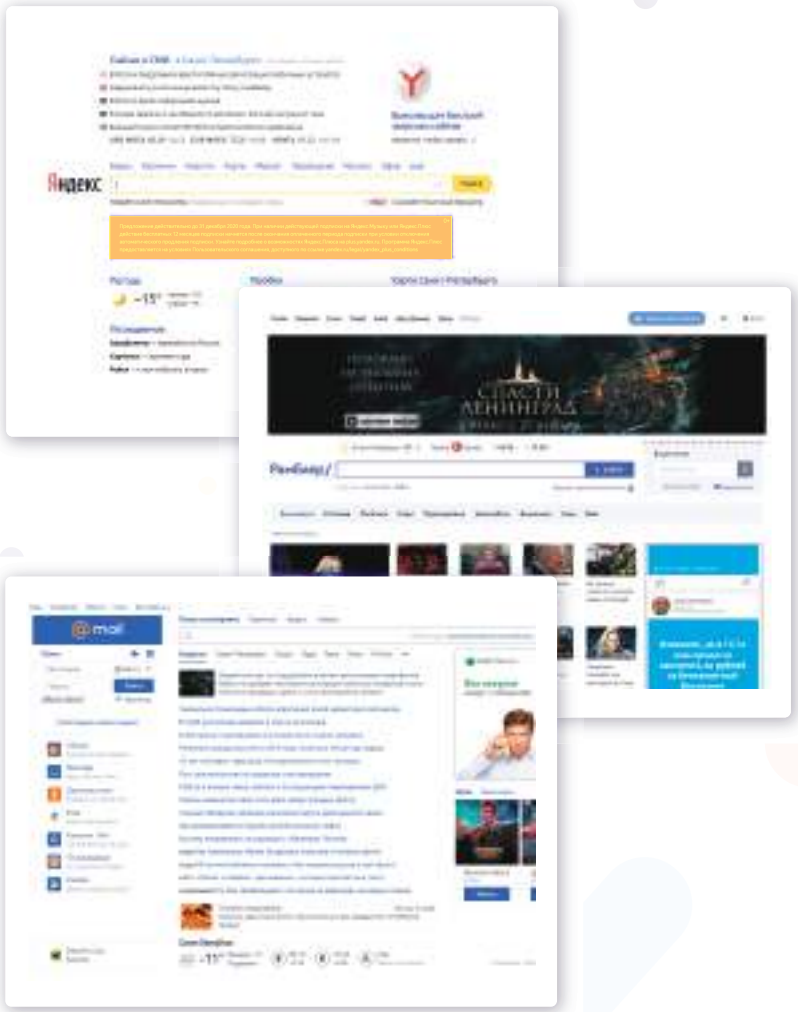
Что относится к персональным данным, а что к личной (конфиденциальной) информации?
Какую информацию можно публиковать в сети?
Почему не стоит публиковать свои полные данные?

Анонимность в сети: правда или вымысел?
Какие правила поведения в сети нужно соблюдать?

Какие опасности подстерегают нас в открытых сетях?
Как не стать жертвой преступника при использовании открытых сетей?
Какие правила пользования чужой техникой нужно помнить?

Лицензионное соглашение/правила пользования: читать или нет?
Почему важно знать правила использования программного продукта/интернет-ресурса?

Виды Интернет-мошенничества (объекты мошенничества)?
Какие виды преступлений распространены в Интернете?
Как не стать жертвой киберпреступника?



Мы давно живем в то время, когда люди для удобства общения и различных переписок используют электронную почту.

В этом разделе мы расскажем Вам о самых популярных службах электронной почты, об их возможностях и о правилах ведения почтового ящика.

Почтовый адрес должен быть **удобен в произнесении** и понятен Вашему собеседнику. Используйте в названии **реальные имя и фамилию,** это позволит облегчить связь с Вами. В названии почты не стоит употреблять посторонние слова, т.к. это может Вас скомпрометировать. Например, если вас зовут **Екатерина Иванова,** то Ваш почтовый ящик следует назвать **KateIvanova** или **EkaterinaIvanova,** если такие почтовые ящики уже существуют, то следует добавить Ваш год рождения или хотя бы две последние цифры (KateIvanova76 или EkaterinaIvanova1976). Согласитесь, что говорить Вашу почту «EkaterinaIvanova1976» не стыдно, в отличие от «Kotenok1976».

ПАРОЛЬ

Ваш пароль **не должен быть простым,** так как простой пароль — наибольшая угроза вашей учетной записи. Обычные слова (marina, begemot), а также предсказуемые сочетания букв (qwerty, 123456) могут быть легко подобраны программами для взлома паролей. Не стоит использовать в качестве пароля общеизвестные данные — имя, день рождения или номер паспорта. Чтобы создать сложный пароль, следует использовать и прописные, и строчные латинские буквы, цифры и знаки пунктуации (допускаются знаки `!@#$%^&*()_=+[]{};:«\|,.<>/?).

Очень хороший вариант для пароля — написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Такой пароль легко запомнить, и в то же время сложно взломать. Например, «вишневый_пирог» в английской раскладке выглядит как «dbiytdsq_gbhju».

Нельзя использовать один и тот же пароль для разных сервисов! Кроме того, пароль необходимо регулярно менять.

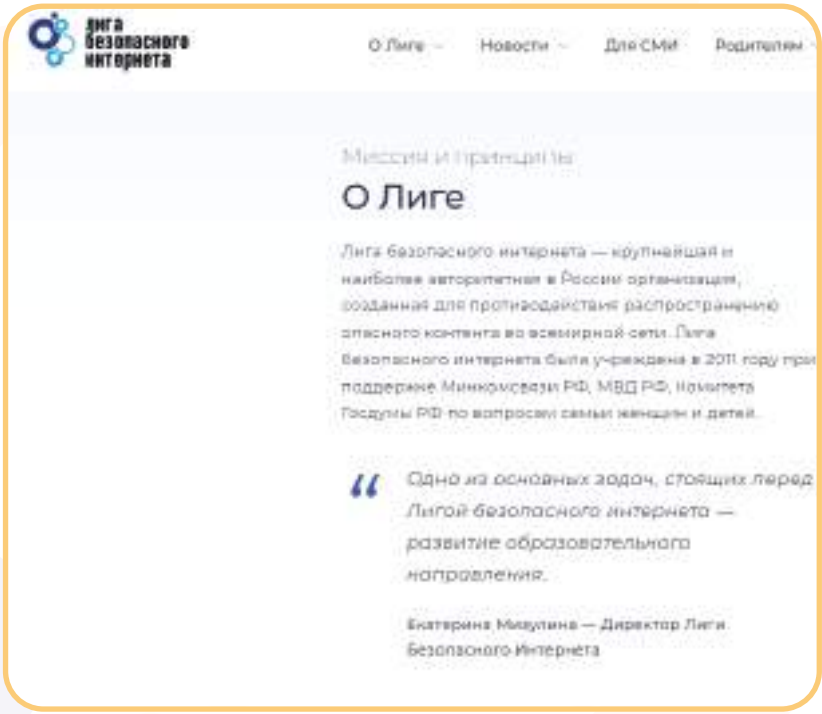
ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА. МЫ ДЕЛАЕМ ИНТЕРНЕТ ЧИЩЕ

Выявляем и блокируем опасный контент, **способствуем** поимке киберпреступников

Поддерживаем полезные сайты и **способствуем** их развитию

Представляем Россию в мире

Обучаем детей и родителей безопасности в сети



Подробнее о нас читайте на сайте: www.ligainternet.ru

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА

Телефон горячей линии

8 800 700 5676

Сайт

найтиребенка.рф
ligainternet.ru

Соцсети

vk.com/liga
vk.com/find_child

t.me/ligainternet
t.me/findchild