10-11 класс

лига безопасного интернета

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ

МАТЕРИАЛЫ К «УРОКУ БЕЗОПАСНОГО ИНТЕРНЕТА»
для учащихся старших классов

БЕЗОПАСНЫЙ ИНТЕРНЕТ

Москва, 2023

Материалы для учащихся средних классов к «Уроку безопасного Интернета»

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

ПРЕДИСЛОВИЕ

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 культуру поведения в сети. Предлагаемые материалы, созданные Лигой безопасного Интернета, могут стать основанием для вашей интенсивной работы и ещё раз привлекут ваше внимание к проблемам агрессивной цифровой среды.

Авторы предполагают наглядный материал для демонстрации на занятии или самостоятельной работы, конкретные советы, включают 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».

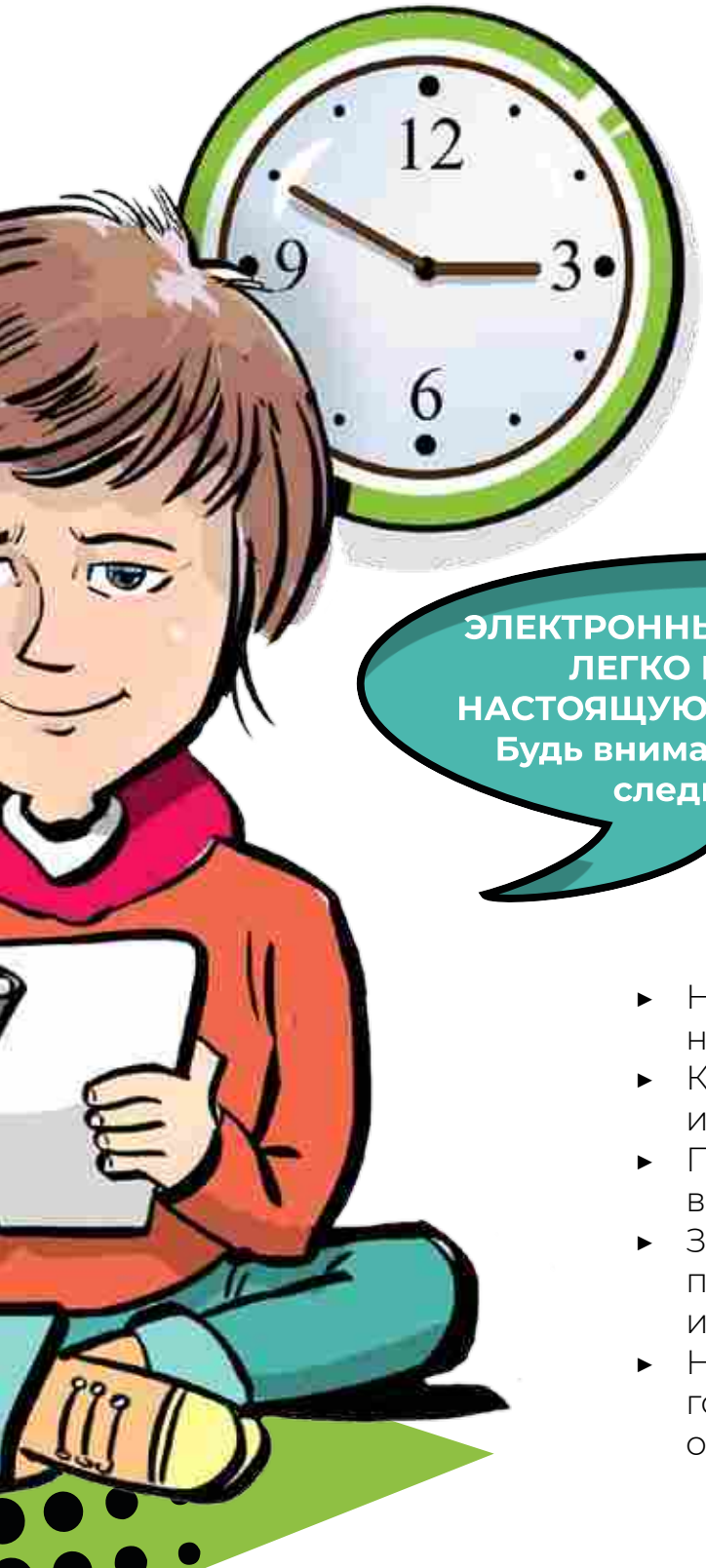
Информация в материалах, такихкак «Мошенничество в Интернете», может стать темой индивидуального образовательного проекта.

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 НАСТОЯЩУЮ ЗАВИСИМОСТЬ. Будь внимателен и старайся следить за собой.

Бей тревогу, если заметил у себя следующие признаки:

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

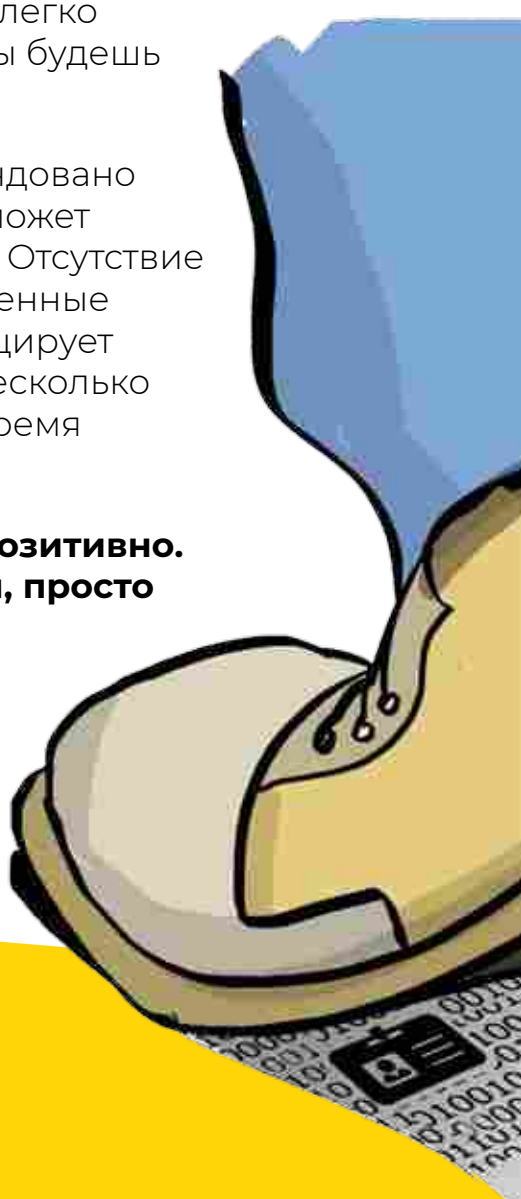
Если ты хочешь избежать Интернет-зависимости, то старайся придерживаться следующих правил:

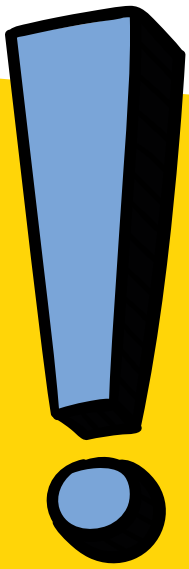
Не бери в руки телефон хотя бы за час до того, как планируешь лечь спать. Интернет, соцсети или игры могут вызвать яркие эмоции, которые помешают уснуть.

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 будешь сожалеть о потерянном свободном времени.

Соблюдай режим отдыха и сна. Детям рекомендовано спать 9-10 часов. Только в таком режиме твой мозг сможет полностью отдохнуть, а организм восстановить силы. Отсутствие правильного режима сна негативно влияет на умственные способности, нервную систему, настроение и провоцирует возникновение ряда заболеваний. Днем старайся несколько часов проводить на свежем воздухе, включая в это время активную физическую нагрузку.

Жизнь надо стараться воспринимать позитивно. Знай, что не существует нерешаемых проблем, просто ты пока не нашел нужного решения.

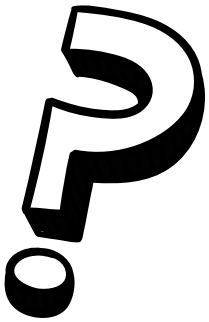




ОБЩАЙСЯ С ДРУЗЬЯМИ В РЕАЛЬНОЙ ЖИЗНИ, А НЕ В ОНЛАЙНЕ!

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.

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:

- Все, что однажды попало в Интернет, остается там навсегда.
- 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.

ЗАПОМНИ!

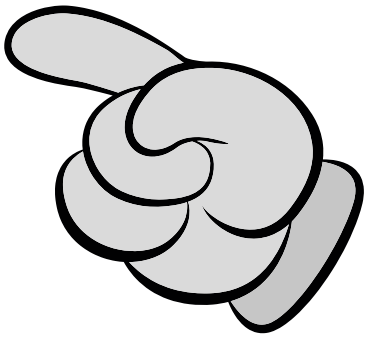
АНОНИМНОСТЬ В СЕТИ – МИФ!

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

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

Подтверждённая страница
Эта отметка означает, что страница подтверждена администрацией VK

ВНИМАНИЕ:
БУДЬ ОСТОРОЖЕН 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.

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.

КАК НЕ СТАТЬ ЖЕРТВОЙ ТРАВЛИ

- Не вступайте в словесные перепалки в комментариях, на форумах, в беседах. У комментаторов может появиться желание мести.
- Чаще меняйте пароли в соц. сетях, так как злоумышленники могут писать от Вашего имени.
- Игнорируйте сообщения, в которых Вас оскорбляют или угрожают. Также стоит уведомить о таких сообщениях администрацию сайта или сервиса.
- Не угрожайте хулигану «найти и наказать». Это лишь усугубит ситуацию.
- Не выкладывайте в сеть лишнюю информацию или файлы, которые могут компрометировать Вас или Ваших знакомых. Не стоит отправлять такую информацию людям, которые не вызывают доверия.
- Не присоединяйтесь, если Ваши друзья дразнят кого-то в сети.
- Попросите их остановиться, предупредите о вредных последствиях травли.
- Удалите злоумышленника из соцсетей, заблокируйте доступ к Вашей странице, добавьте в черный список.
- Поговорите с родителями или учителями об этой ситуации. Они не оставят Вас одного в неприятном состоянии и помогут наилучшим способом разрешить любую ситуацию.
- Вместе с родителями соберите доказательства: сделайте скриншоты переписки, скопируйте ссылки на аккаунты обидчика, Вам это может пригодиться в случае обращения в полицию.

ОБЩЕНИЕ В ИНТЕРНЕТЕ

Интернет – это возможность общаться с друзьями на расстоянии, не терять связь на летних каникулах и обсуждать интересные темы. Но 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.

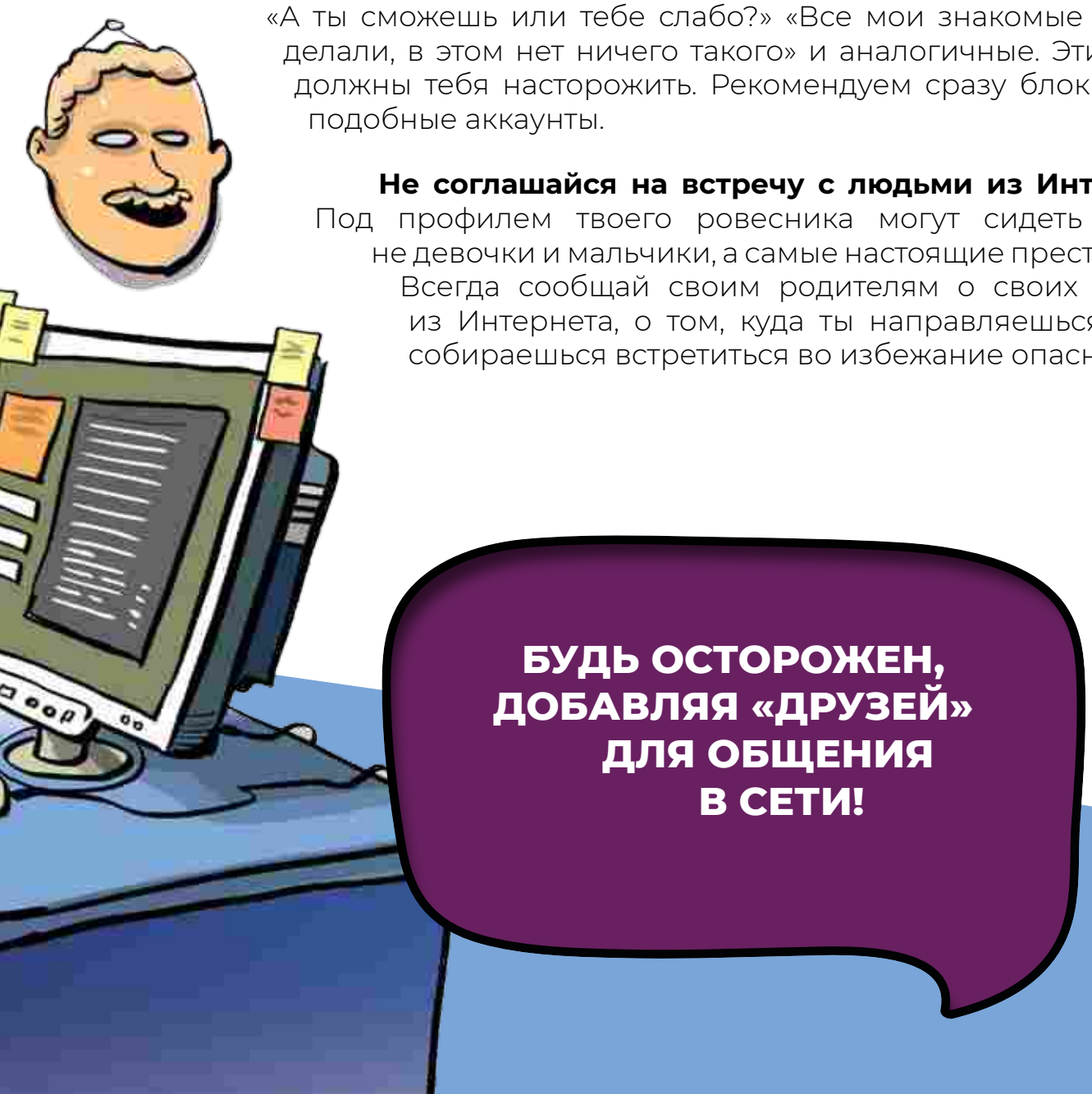
ГЛАВНЫЕ ПРАВИЛА ОБЩЕНИЯ С НЕЗНАКОМЦАМИ В ИНТЕРНЕТЕ

Страницы в социальных сетях лучше закрыть от посторонних. Если ты не знаешь, как это сделать, то попроси родителей тебе помочь. Это защитит твои персональные 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.

Будь осторожен, когда добавляешь незнакомого человека в друзья, если ты не знаешь его в реальной жизни. Если новый знакомый задает тебе много вопросов о семье и о том, где ты живешь или учишься, то не рассказывай ему эту информацию и сразу сообщай освоим родителям.

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

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, о том, куда ты направляешься, с кем собираешься встретиться во избежание опасности.



БУДЬ ОСТОРОЖЕН, ДОБАВЛЯЯ «ДРУЗЕЙ» ДЛЯ ОБЩЕНИЯ В СЕТИ!

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Персональные данные – все данные о человеке, своего рода «паспорт его личности». Их раскрытие в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже денег и документов, аккаунтов, различным мошенническим действиям.

ЧТО ОТНОСИТСЯ К ПЕРСОНАЛЬНЫМ ДАННЫМ

- **Фамилия, имя, отчество;**
- **Все твои документы** (паспорт, свидетельство о рождении, аттестат);
- **Банковские данные** (номер счета, карты, пин-код, CVV-код);
- **Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы);
- **Фотографии и видеозаписи с твоим изображением;**
- **Данные о твоих родственниках;**
- **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»

80% преступников берут информацию в соц. сетях

Личная информация используется для кражи паролей

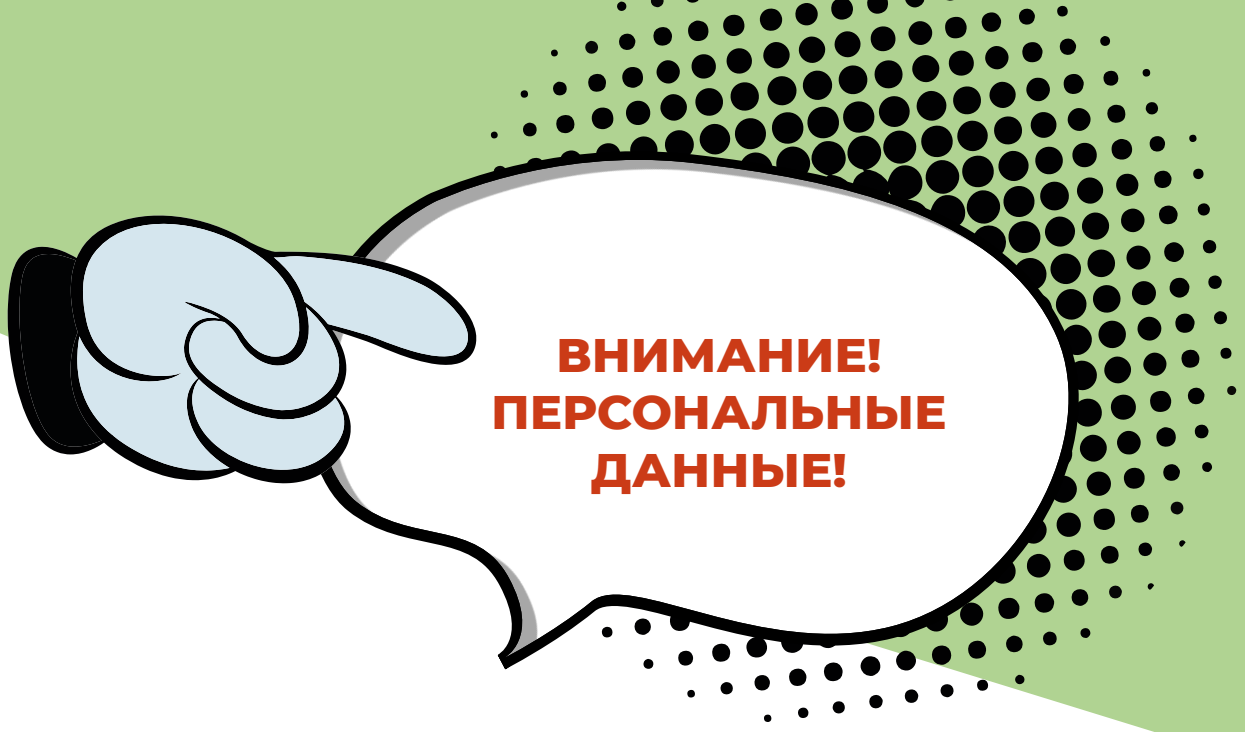
Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг, хищение!

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	Все пользователи
Кто может видеть моих скрытых 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 И 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.



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

ОСТОРОЖНО, ПОДДЕЛКА

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

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

КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ?

- Просят подтвердить логин/пароль
- Предлагают скачать по ссылке бесплатное ПО
- Просят отправить СМС (платно)
- Просят прислать данные банковской карты

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!

ОСТОРОЖНО, СПАМ

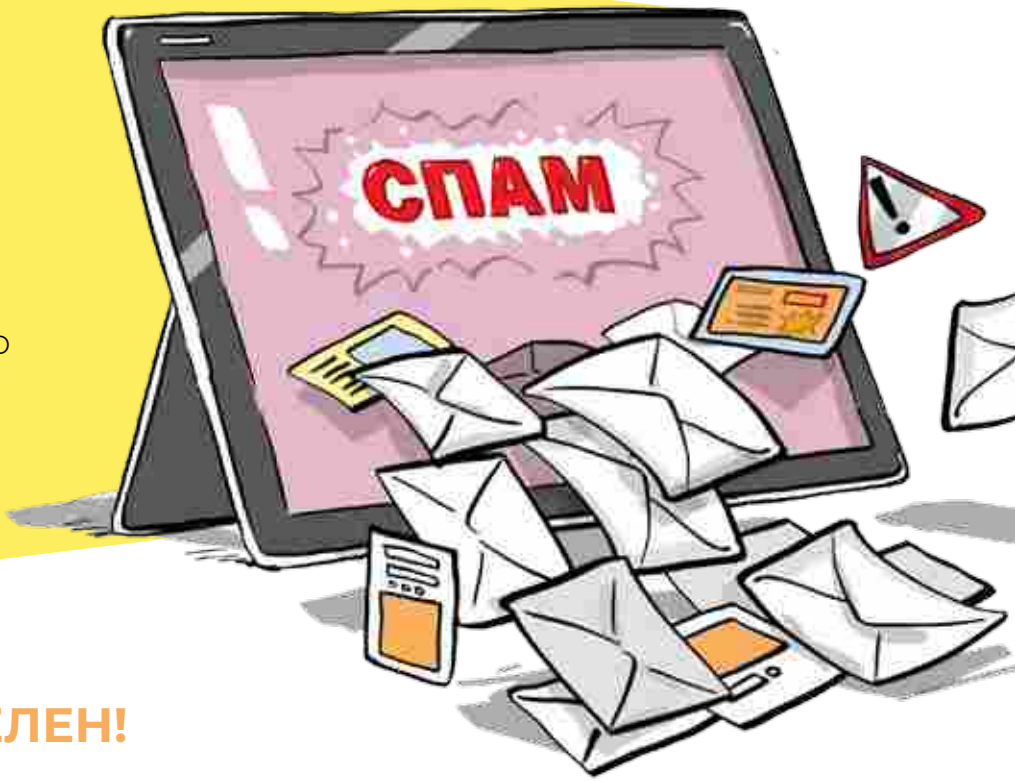
Спам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания

Первоначально слова «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:

- Оплатить навязчивую услугу
- Получить платную подписку на ненужную информацию
- Потерять учетные и (или) иные данные
- Стать жертвой обмана



БУДЬ ВНИМАТЕЛЕН!

- Настрой безопасность браузера и почтовой программы (отключи 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 соглашение 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!

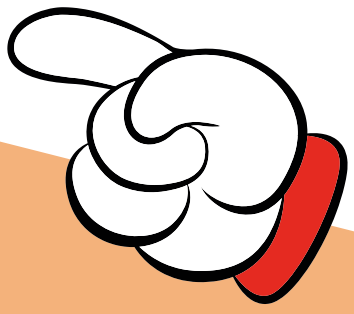
ПОДТВЕРЖДАЯ СОГЛАШЕНИЕ «ВСЛЕПУЮ», ТЫ МОЖЕШЬ:

- 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

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!

ОСТОРОЖНО, МОШЕННИКИ

ПРЕДУПРЕЖДЕН — ЗНАЧИТ, ВООРУЖЕН

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

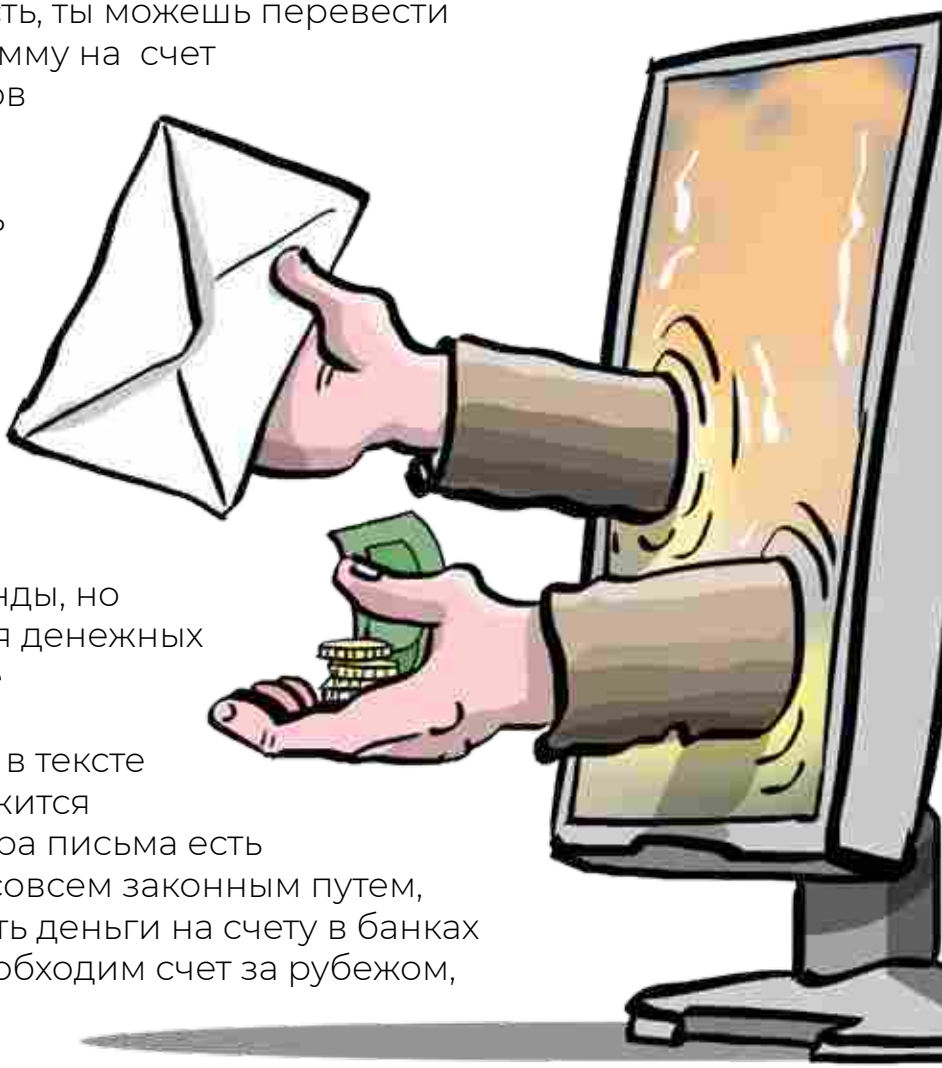
КАРДИНГ И ФИШИНГ

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 свой стороны. Ему срочно необходим счет за рубежом, куда можно перечислить деньги. Авторы подобных писем попросят тебя обналичить крупную 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 денежные средства.

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ КРЕДИТНЫМИ КАРТАМИ В СЕТИ ИНТЕРНЕТ

Всегда следует обращаться аккуратно со своими зарплатными, кредитными, дебетовыми картами, на которых есть доступные для списания средства. Для покупок через Интернет лучше открыть отдельную карту, на которую ты будешь переводить определенную сумм денег с основных карт.

Не упускай 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 действия.

Следи за остатком на карте. Предпочтительно проверить баланс через специальную услугу SMS- информирования. Если ты вовремя заметил, транзакцию, которую ты не совершал или совершил ошибочно, ее можно отменить, подав соответствующую заявку.

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

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

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

6 ПРОСТЫХ ПРАВИЛ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

Если ты решил проверить баланс своей кредитной карты онлайн, оплатить счета, перевести деньги кому-либо, купить или продать что-нибудь в Интернете, то эти 6 правил помогут тебе не потерять деньги.

- Своевременно проверяй обновления ПО. Обязательно установи антивирусное ПО. Защити свой wi-fi роутер пароль и используй usb-накопители с осторожностью.
- ТОЛЬКО СЛОЖНЫЕ ПАРОЛИ
- Самые эффективные пароли – написать русское слово 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 запоминающиеся для форумов и других, не представляющих опасности для ваших денег. Храните свои пароли в секрете. Не отправляйте их по SMS, e-mail, мессенджерах и соц. сетях.

НЕ ПЕРЕХОДИ ПО ССЫЛКАМ.

НАБИРАЙ АДРЕС САЙТА САМОСТОЯТЕЛЬНО.

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

УСТАНОВЛЕНО ЛИ ЗАЩИТНОЕ СОЕДИНЕНИЕ?

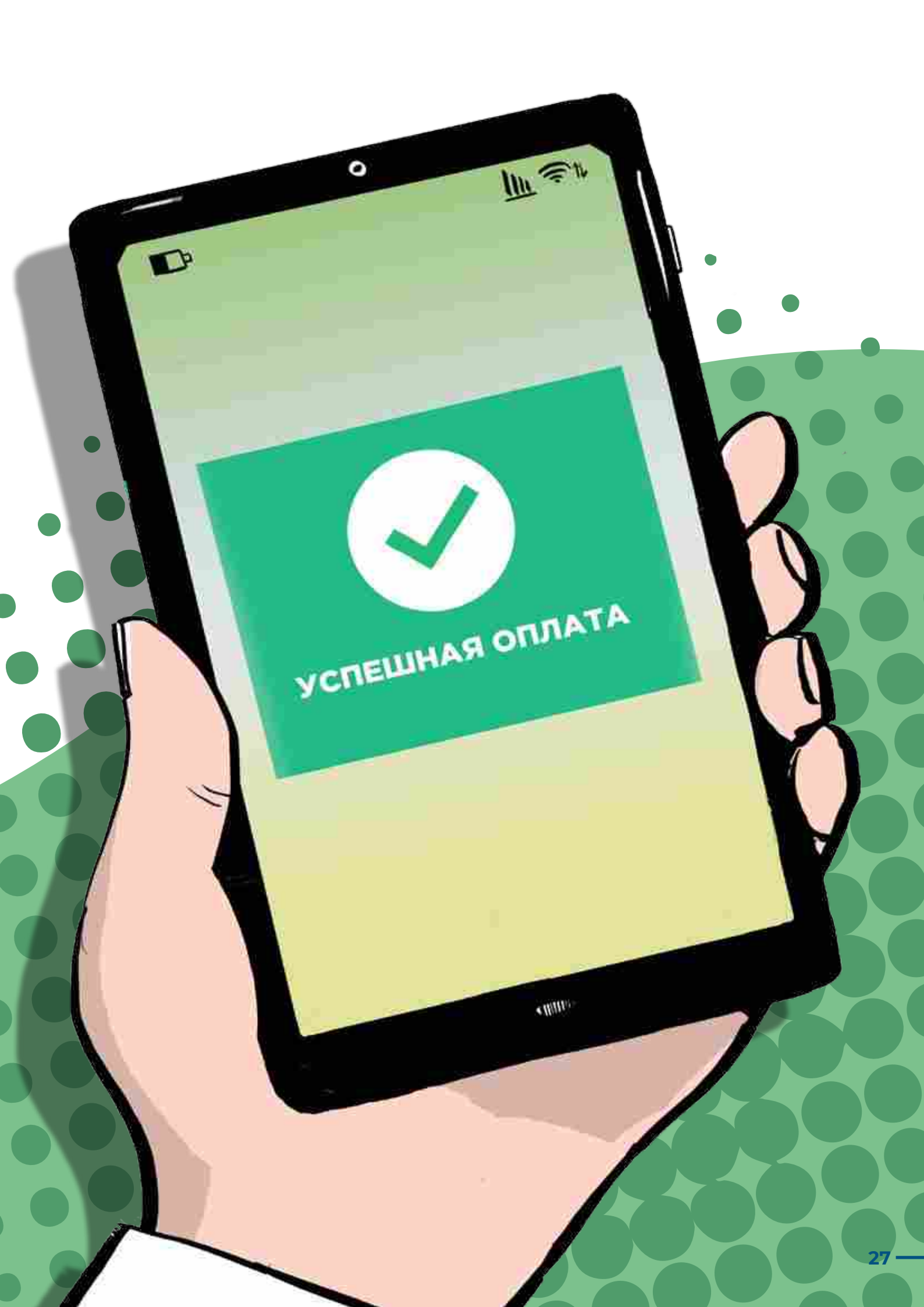
В СЕТИ Интернет используются два протокола: HTTP и Secure HTTP. Прежде чем ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), обрати внимание на адресную строку, убедитесь, что имя протокола имеет вид https://, а не http («s» — значит secure, англ. «защищенный»).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

ТРАНЗАКЦИИ ТОЛЬКО НА ДОМАШНЕМ КОМПЬЮТЕРЕ.

Никогда не проверяй баланс личного счета, не оплачивай счета, не совершай 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 wi-fi.

ПРИДЕРЖИВАЙСЯ ЗДРАВОГО СМЫСЛА

Чтобы защитить себя от мошенников, тщательно изучай эти простые правила. Внимательно отнесись к оповещениям из своего «банка». Часто злоумышленники присылают сообщения, в которых написано, что ваш счет будет заблокирован, если ты не предпримешь немедленных действий, связанных с переводом денег, или представляются твоим родственниками или друзьями и требуют денег на проведение операции.


УСПЕШНАЯ ОПЛАТА

ДЕСТРУКТИВНЫЕ СООБЩЕСТВА В СЕТИ – ПРОБЛЕМА РЕАЛЬНОГО МИРА

В Интернете существует большое количество опасных групп и сообществ, которые распространяют опасные для жизни, здоровья и нравственности человека идеологию, увлечения, в том числе, вовлекают в экстремистскую деятельность и совершение иных преступлений.

К таким группам относятся:

- Группы, в которых публикуется контент, связанный, с тематикой самоубийств (суицидальные).
- Группы, распространяющие идею и практики причинения самому себе физического или психологического вреда (аутодеструктивные).
- Сообщества по криминальной идеологии – продвигают идеалы из криминальной среды среди подростков.
- Сообщества по пропаганде наркотиков – пропагандируют употребление наркотиков, вовлекают своих членов даже в распространение запрещенных веществ.
- Экстремистские сообщества – пропагандируют экстремистские идеи, а также привлекающие своих подписчиков к совершению преступлений на почве политики, расовой, национальной или религиозной ненависти.

ПОСЛЕДСТВИЯ УЧАСТИЯ В ДЕСТРУКТИВНЫХ И ОПАСНЫХ СООБЩЕСТВАХ:

- Выраженное стремление к разрушению и деструктиву.
- Снижение успеваемости в школе.
- Нарушение коммуникации и конфликты со сверстниками.
- Неуважительное отношение ко всем взрослым.
- Попытки самоубийства и причинения себе вреда.
- Под влиянием опасных сообществ, его участники могут шантажом или обманом быть втянуты в преступную деятельность.

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

Собеседник (вербовщик) в Интернете:

- Пытается завладеть всем твоим вниманием и временем.
- Приглашает в сообщества с очень узкими интересами (не обязательно закрытое).
- Регулярно выдает тебе «задания». Например: облейся холодной водой, напиши пост и поставь правильный хештег, опубликуй свои фото в конкретных условиях и т.п. Такие активности «дрессируют» пользователей на бездумные массовые действия.
- Награждает за выполнение заданий в соцсетях, сетевых сообществах и массовых играх. Это мотивирует пользователей участвовать в активности не «просто так», а за награду, даже если она виртуальная.

ОПАСНЫЕ ПУБЛИКАЦИИ

Время от времени в Интернете ты можешь сталкиваться с материалами, фото, видео или публикациями, которые тебе неприятны, вызывают беспокойство, оскорбляют или расстраивают тебя. Возможно, ты уже сталкивался в Интернете с таким контентом.

ЧТО ЭТО МОЖЕТ БЫТЬ:

- Публикации, пропагандирующие агрессию, насилие по отношению к другим.
- Публикации, пропагандирующие причинение вреда другим людям или даже себе.
- Материалы, разжигающие рознь на этнической, религиозной, национальной или расовой почве.
- Шок-контент – материалы, содержащие большое количество отвратительного, неприятного, ужасного контента.
- Пропаганда опасных для жизни, вредных для здоровья и противозаконных увлечений. К ним могут относиться некоторые экстремальные и травмоопасные развлечения, пропаганда употребления наркотиков.

ЧТО ДЕЛАТЬ?

- Обратиться 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 и нажми «Пожаловаться» в его аккаунте.

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 online всегда и везде, а социальные сети превращаются в устойчивую привычку, без которой мы уже не можем предоставить 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 социальные 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

В контексте соц. сетей «липовыми» страницами называют поддельные страницы реальных людей с идентичными фотографиями и данными.

Как отличить «липу» от оригинала?

Существует несколько признаков «липовых» страниц.

1. Фотографии, «вырванных» из других соц. сетей или поисковых сервисов. Когда ты выкладываешь фотографию, многие соц. сети помечают ее своим логотипом или скачать ее из сервиса без него невозможно. При скачивании таких фото теряется качество. Если ты заметил, что в профайле VK много фотографий из «одноклассников» и их качество оставляет желать лучшего, вполне вероятно, что страница липовая.«Пустой» профайл. Обычно создатели «липовых» страниц не особо стараются повторить оригинал» не указывают личную информацию, интересы и т.д. Если никаких данных, кроме имени, не указано, стоит насторожиться.

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

3. Если страница создана пару дней назад, а все фотографии загружены одной датой – это тоже, вероятнее всего «липовая» страница.

4. От «липовых» страниц приходит много СПАМа, так как многие мошенники создают их для накрутки голосов или приглашения людей на свои ресурсы.

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

6. Если указана школа/ВУЗ и год окончания, проверь, есть ли в друзьях люди из этой школы/ВУЗа. Напиши им, спроси, знакомы ли вы с этим человеком лично.

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

Страничка в соц. сетях – мощный инструмент формирования имиджа человека,

поэтому так необходимо внимательно относиться к тому, как она выглядит.

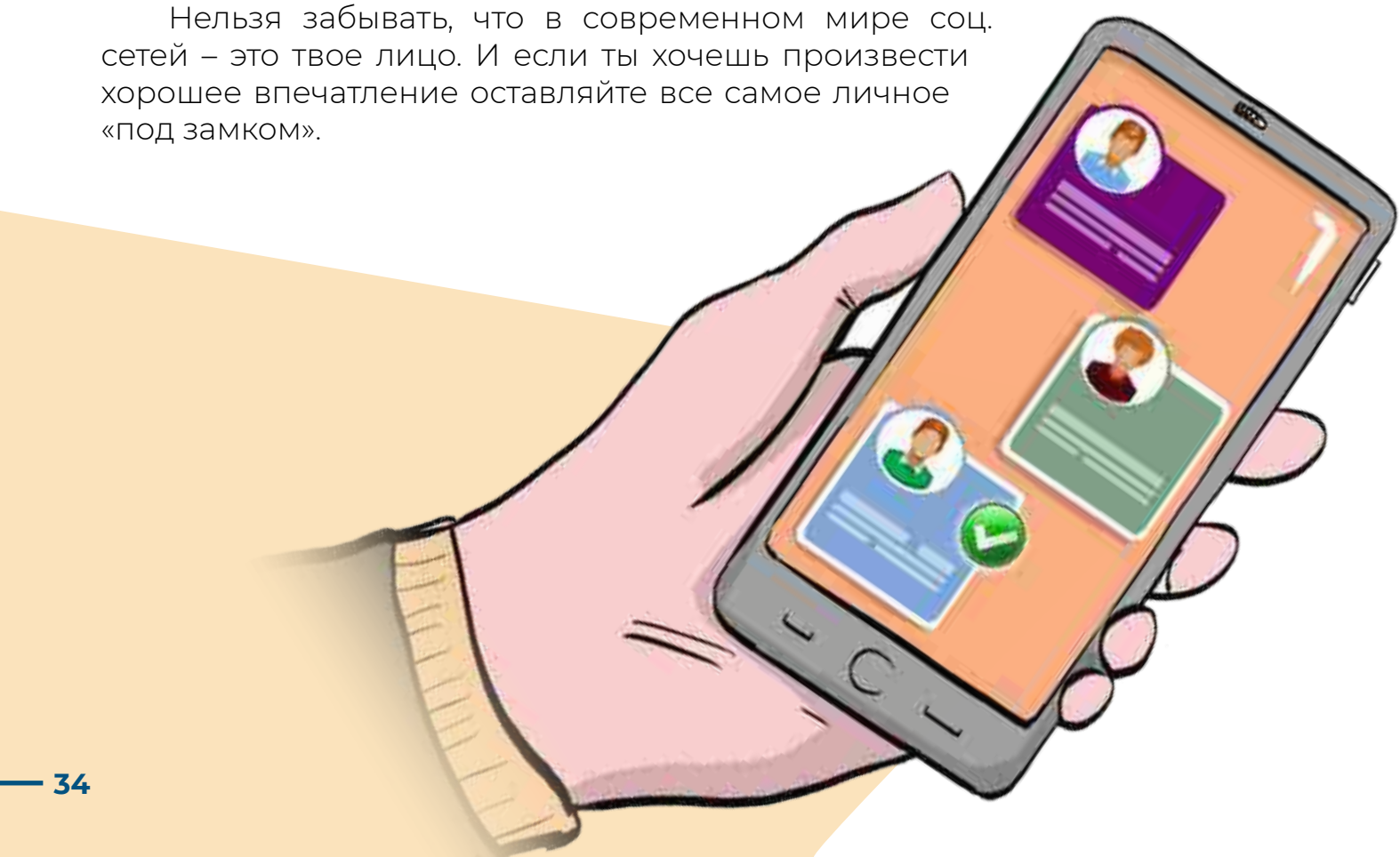
Но как найти эту грань между излишней скрытностью и чрезмерным хвастовством?

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

Если у тебя «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. сетей – это твое лицо. И если ты хочешь произвести хорошее впечатление оставляйте все самое личное «под замком».



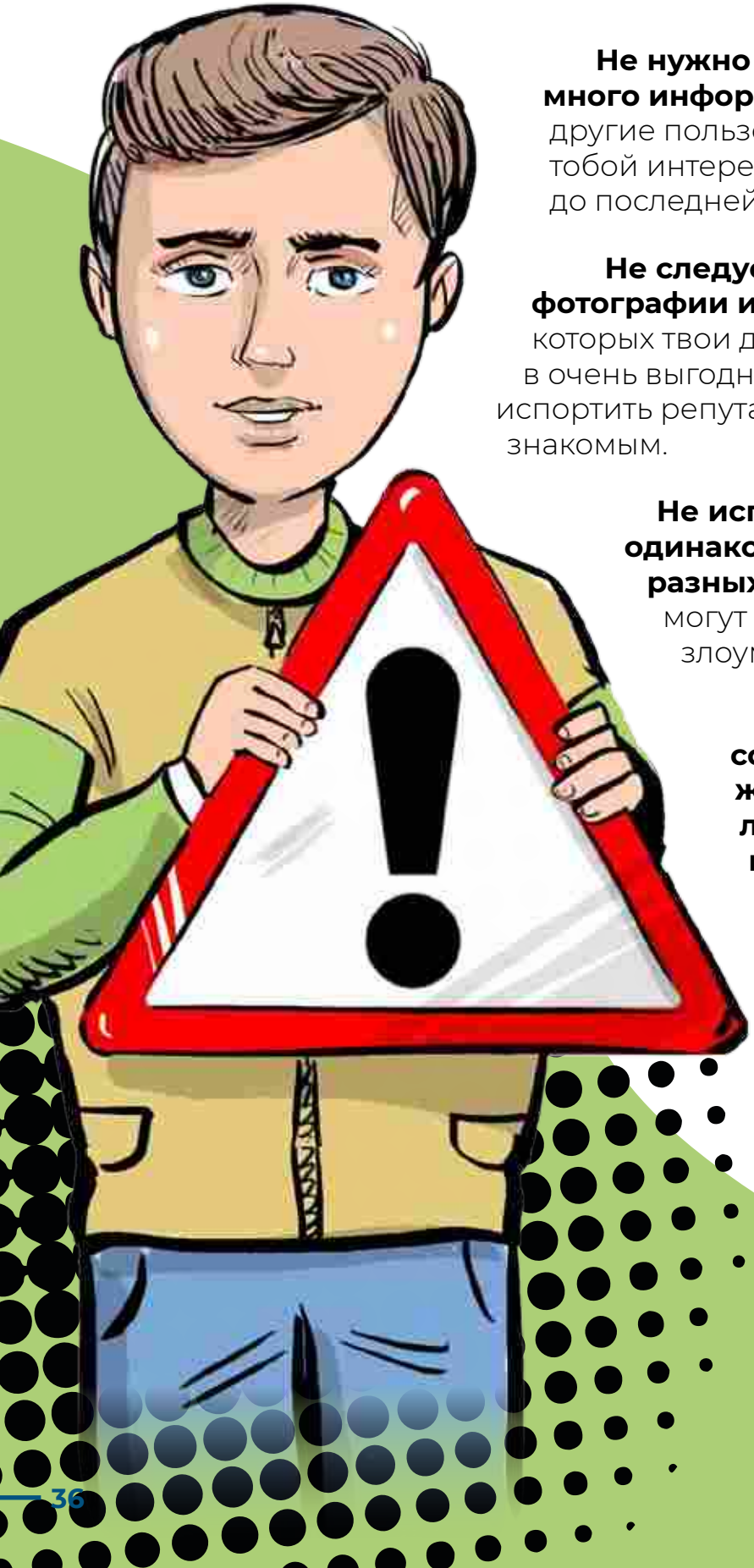
СОЗДАЕМ СВОЮ «СТРАНИЧКУ»

Для регистрации в любой социальной сети тебе понадобится адрес электронной почты. Указывай существующий e-mail, так как с помощью его вам нужно будет подтвердить вашу личность. Обычно администрация сайта присылает письмо на подтверждения регистрации.

Помимо электронной почты для регистрации нужно придумать логин, который будет легко подобрать, и тогда персональные данные могут попасть в руки злоумышленников. Не указывай в качестве пароля дату своего рождения, используй помимо цифр буквы с разным регистром.

После регистрации тебе будет предложено заполнить профиль: указать краткую информацию о себе, дату рождения, интересы, место работы/учебы и так далее. Также ты можешь загрузить фотографию профиля – аватар. Не стоит указывать личные данные и размещать фотографии, которые в дальнейшем могут тебя скомпрометировать.

ОСНОВНЫЕ ПРАВИЛА ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ



Не нужно указывать слишком много информации. Помни, что другие пользователи, которые тобой интересуются, прочитают все до последней буквы.

Не следует выкладывать фотографии или медиафайлы, на которых твои друзья показаны не в очень выгодном свете: ты можешь испортить репутацию не только себе, но и знакомым.

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

Старайся писать сообщения без использования жаргонной и ненормативной лексики, с соблюдением правил орографии и пунктуации. Общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, руководством 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 по ьзователей, 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.

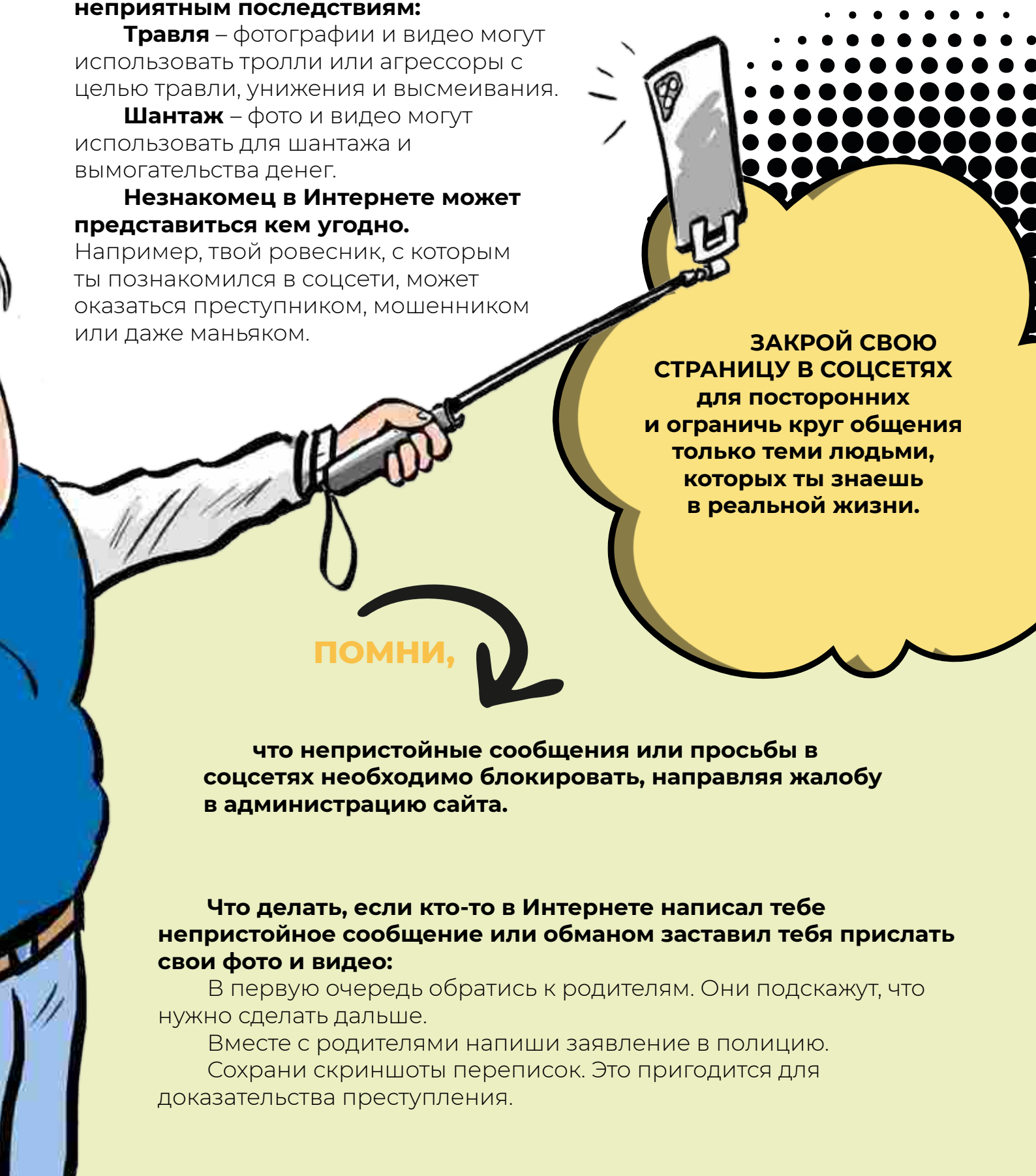
ОБМЕН ФОТОГРАФИЯМИ

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.



ЗАКРОЙ СВОЮ СТРАНИЦУ В СОЦСЕТЯХ для посторонних и ограничь круг общения только теми людьми, которых ты знаешь в реальной жизни.

ПОМНИ,

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

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.

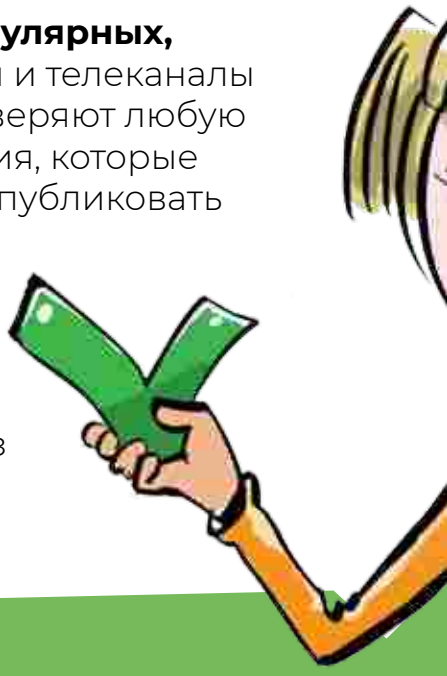
Сохрани скриншоты переписок. Это пригодится для доказательства преступления.

МАНИПУЛЯЦИЯ В ИНТЕРНЕТЕ

В Интернете есть много интересного, веселого и познавательного контента. Но необходимо подвергать сомнению все, что мы читаем и смотрим в Интернете. Фейк – целенаправленно распространяемая ложная информация, которую специально создают, чтобы запутать, ввести в заблуждение или посеять панику среди людей.

Оригинал всегда лучше любого пересказа. Очень важно искать оригинальный источник новости. Подумай, можешь ли ты доверять этому источнику? Если это «желтое СМИ» или сайт, специально собирающий громкие заголовки, то доверять такому источнику нельзя!

Обрати внимание на текст. У реальной новости всегда много свидетелей и участников, которые рассказывают о событиях своими словами. По этой причине разные СМИ напишут про одну и ту же новость по-разному. Фейки – наоборот, не отличаются разнообразием. Фейковые новости, даже опубликованные на разных сайтах, мало отличаются друг от друга, а иногда и вовсе могут быть написаны «под копирку». Фейк придуман одним источником, откуда его скопировали другие сайты.



Настоящая новость никогда не пройдет мимо популярных, известных и авторитетных СМИ. Крупные газеты, сайты и телеканалы беспокоятся о своей репутации, поэтому тщательно проверяют любую информацию. Фейки распространяют небольшие издания, которые могут не проверить информацию, а иногда и заведомо опубликовать ложные сведения.

Проверяй факты и цитаты из новости. Не важно, кому принадлежит цитата, насколько это уважаемый и популярный человек. Недобросовестные СМИ могут подделать или вырвать из контекста любые слова для создания фейковой новости.

ЕСЛИ ТЫ НАШЕЛ ИЛИ ПОЛУЧИЛ НЕДОСТОВЕРНУЮ ИНФОРМАЦИЮ, НЕ ПЕРЕСЫЛАЙ ЕЕ ДРУЗЬЯМ И РОДНЫМ! СНАЧАЛА ДОЖДИСЬ ОФИЦИАЛЬНОГО ОПРОВЕРЖЕНИЯ ИЛИ ПОДТВЕРЖДЕНИЯ.

ПРОВЕРКА ФАКТОВ И ПОИСК ИСТИНЫ

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

- **Необходимо обратить внимание на источник информации,** поскольку одним из доказательств достоверности является наличие ссылок на источники.
- **Свидетельства очевидцев** – один из самых сложных методов проверки достоверности. Обрати внимание, подтверждает ли очевидец тезисы, о которых нам сообщает журналист.
- **Если в качестве доказательства достоверности тебе предоставляют фото, необходимо убедиться, что изображение действительно имеет отношение к описанным событиям.** Для этого мы рекомендуем найти данную новость на интернет-ресурсах и воспользоваться сервисами Google или Яндекс «поиск по картинкам», далее следует обратить внимание на первоисточник и дату публикации, соотнести с источником информации.

- **Ты хочешь проверить подлинность видео,** перейдите на сайт YouTube, RuTube, кликнув по логотипу в нижнем правом углу, прочти описание к видео, посмотри, когда и кем данное видео было загружено, а также обрати внимание на детали: номера машин, название улиц.

МЕТОДЫ ОЦЕНКИ ИСТОЧНИКОВ ИНФОРМАЦИИ

Необходимо убедиться в компетенции источника, разбирается ли он в данном вопросе.
Если информация получена из Интернета, проверь регистрацию ресурса как СМИ, иначе он имеет полное право публиковать любые «новости». Выясни 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 знает, либо скрывает имена конкретных людей, лабораторий и ВУЗов. Таким сообщениям нельзя доверять, так ка под прикрытием «ученых» можно рассказывать абсолютно любые небылицы и запутывать неопытных читателей.

«На протяжении длительного времени они изучали анамнез и истории пятисот тысяч человек. Выяснилось, что побочным эффектом употребления поливитаминов может стать рак. Но это касается людей, которые придерживаются нормального пищевого рациона и одновременного 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 критика и неодобрение 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 оправдывает возложенных на них надежд, а часто даже усугубляет болезни и провоцирует новые».

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

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)**

ПРЯМЫЕ ТРАНСЛЯЦИИ И ВИДЕОХОСТИНГИ

Видеохостинги – специальные сайты, где пользователи могут загружать и просматривать видео, делиться ими со своими друзьями. С помощью видеохостингов любой пользователь, в том числе ребенок или подросток, получает доступ к огромному количеству разнообразного контента.

Среди миллионов видео, которые ежедневно загружаются на видеохостинги, присутствует большое количество опасного, деструктивного и неприемлемого контента.

НЕ ПОЗВОЛЯЙ МАНИПУЛИРОВАТЬ СОБОЙ!
НЕ ВЕРЬ ВСЕМУ, ЧТО ПИШУТ В ИНТЕРНЕТЕ!

ЧЕМ ОПАСНЫ ВИДЕОХОСТИНГИ?

- На многих сайтах обмена видео нет возможности ограничить круг лиц, которые могут смотреть видео, загруженные пользователем.
- Как и в случае с онлайн-трансляциями, в записанных видео можно случайно выдать личную информацию.
- Функция комментирования видео дает пользователям возможность писать неуместные и оскорбительные сообщения.
- Рекомендательные алгоритмы видеохостингов показывают пользователю деструктивные и противоправные видео, даже если пользователь не интересуется этой тематикой.
- Опасные видеоматериалы делают зрителей агрессивными и повышают риск возникновения психических расстройств.
- Видеохостинги формируют зависимость от просмотра видео, «затягивают» настолько сильно, что человек теряет счет времени и не может отличить реальную жизнь от виртуальной.

Самый популярный видеохостинг в России и в мире – «YouTube». Именно он представляет наибольшую опасность для жизни, здоровья и психики. Опасный контент на YouTube не удаляется и намеренно продвигается среди пользователей в России.

В 2021 году американские исследователи обнаружили, что рекомендательные алгоритмы YouTube предлагают пользователям видеоролики, которые нарушают собственные правила онлайн-площадки. Согласно данным эксперимента, подобные материалы составили 71% от общего количества просмотренных участниками исследования видео.

Обязательно спроси у родителей, какую информацию нельзя рассказывать и показывать в своих видео.

Помни о необходимости настройки и защиты конфиденциальности своего аккаунта. Личные видео, не предназначенные для чужих глаз, лучше вовсе не публиковать.

Все, что ты публикуешь, в том числе и видео, так или иначе попадает в публичный доступ, где его могут увидеть не только твои друзья, но и вся школа, все родственники, друзья родственников, и даже родители одноклассников. Если ты сомневаешься, хочешь ли ты, чтобы все эти люди увидели это видео, то лучше его не публиковать.

Ознакомься с правилами видеохостинга, узнай, как отправить жалобу в службу поддержки на неприемлемые видео и оскорбительные комментарии.

ОНЛАЙН-ИГРЫ

В умеренных количествах, игры - отличный способ расслабиться и провести время с друзьями онлайн. Но многие онлайн-игры специально затягивают своих пользователей, чтобы те играли как можно дольше. Поэтому бывает так трудно оторваться от игры.

ПРИЗНАКИ ТОГО, ЧТО ТЫ СЛИШКОМ МНОГО ВРЕМЕНИ ПРОВОДИШЬ ЗА ИГРАМИ:

- Ты играешь в онлайн-игры по ночам.
- После игры тебе трудно заснуть.
- Тебе не хватает времени на учебу, выполнение домашних заданий, общение с друзьями и хобби.
- Во время игры ты часто злишься, воспринимаешь все очень эмоционально. Иногда можешь швырнуть что-нибудь в сторону.
- Ты очень злишься, когда проигрываешь.
- Тебе трудно сосредоточиться на чем-либо, кроме игры.

Если ты ответил «да» хотя бы на один из этих пунктов, то, скорее всего, ты тратишь на игры слишком много времени.

Обратись за помощью к родителям. Спроси у них, как можно сократить время игры, установить для себя правила и постараться их придерживаться.

Кроме зависимости, в онлайн-играх тебя могут поджидать и другие опасности. Среди тысяч игроков могут скрываться мошенники и преступники, которые могут попытаться украсть твои персональные данные, деньги или втянуть тебя самого в преступную деятельность.


GAME
UPLOADING

КАКИЕ ОПАСНОСТИ ЕСТЬ В ОНЛАЙН-ИГРАХ:

Многие игры имеют функцию чата. Это означает, что каждый пользователь может прислать тебе ссылку на сторонний ресурс, где ты можешь подхватить компьютерный вирус.

Чаще всего чаты в играх плохо модерируются. А значит любой пользователь может вести себя агрессивно по отношению к тебе, оскорблять или унижать.

Некоторые игры используют GPS и постоянно собирают информацию о местоположении игрока. А это значит, что и другие участники игрового сообщества могут узнать, где ты находишься в данный момент.

- Узнай, есть ли в игре функция чата. Лучше отключить ее, если есть такая возможность.
- Общайся в играх только с теми людьми, которых знаешь лично – с друзьями и знакомыми.
- Не переходи по ссылкам, которые тебе присылают незнакомые люди в чатах.
- Узнай, есть ли в игре модерация. Если кто-нибудь будет грубить или оскорблять тебя, то на него можно будет направить жалобу модератору.

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. Анонимность в сети – МИФ. Все, что мы выкладываем в Интернете, остается там навсегда.

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.

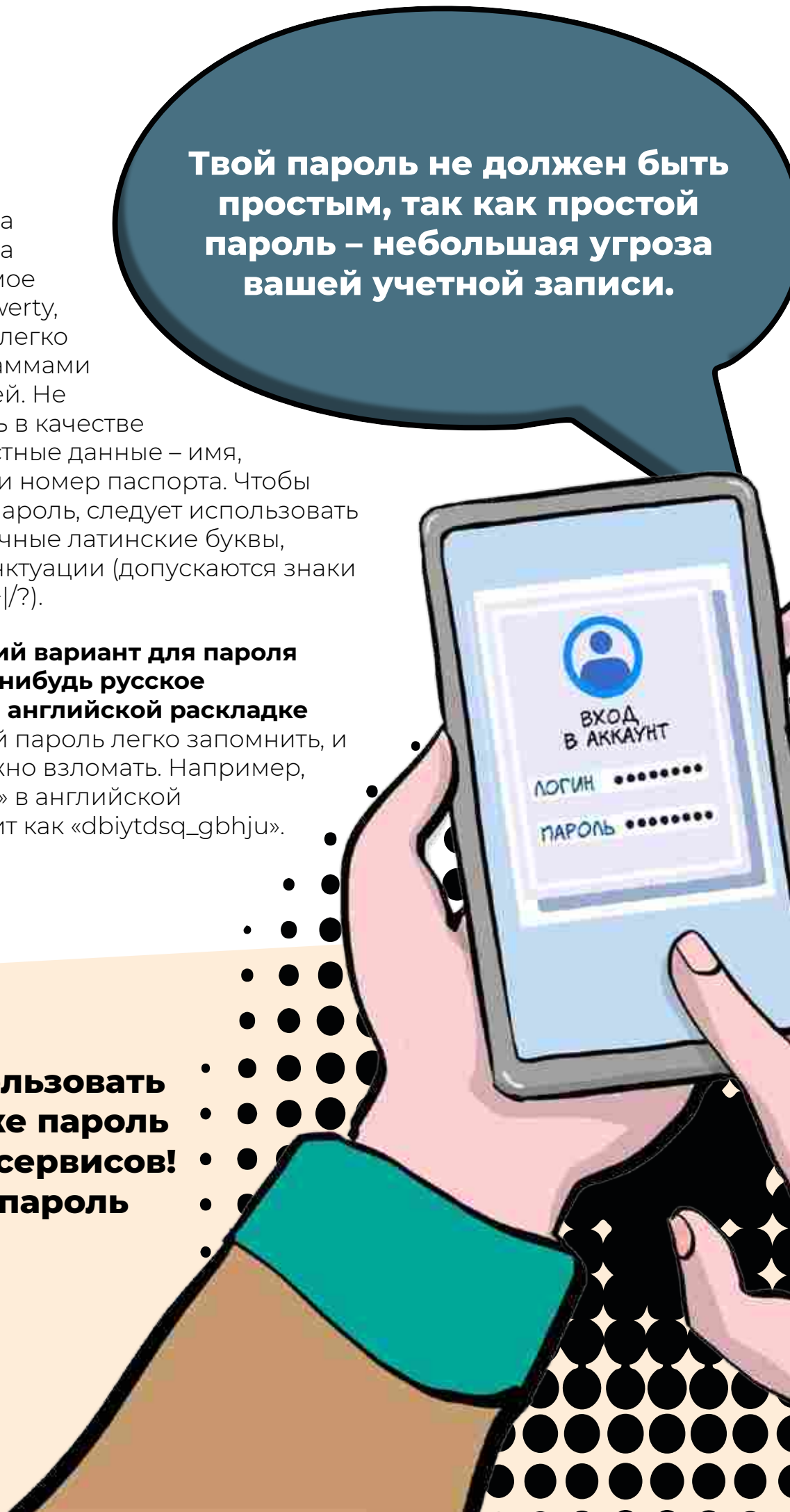
10. Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни. Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

ПАРОЛЬ

Твой пароль не должен быть простым, так как простой пароль – небольшая угроза вашей учетной записи.

Обычные слова (marina, begemot), а также предсказуемое сочетание 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 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.

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

ЛИГА БЕЗОПАСНОГО ИНТЕРНЕТА. МЫ ДЕЛАЕМ ИНТЕРНЕТ ЧИЩЕ

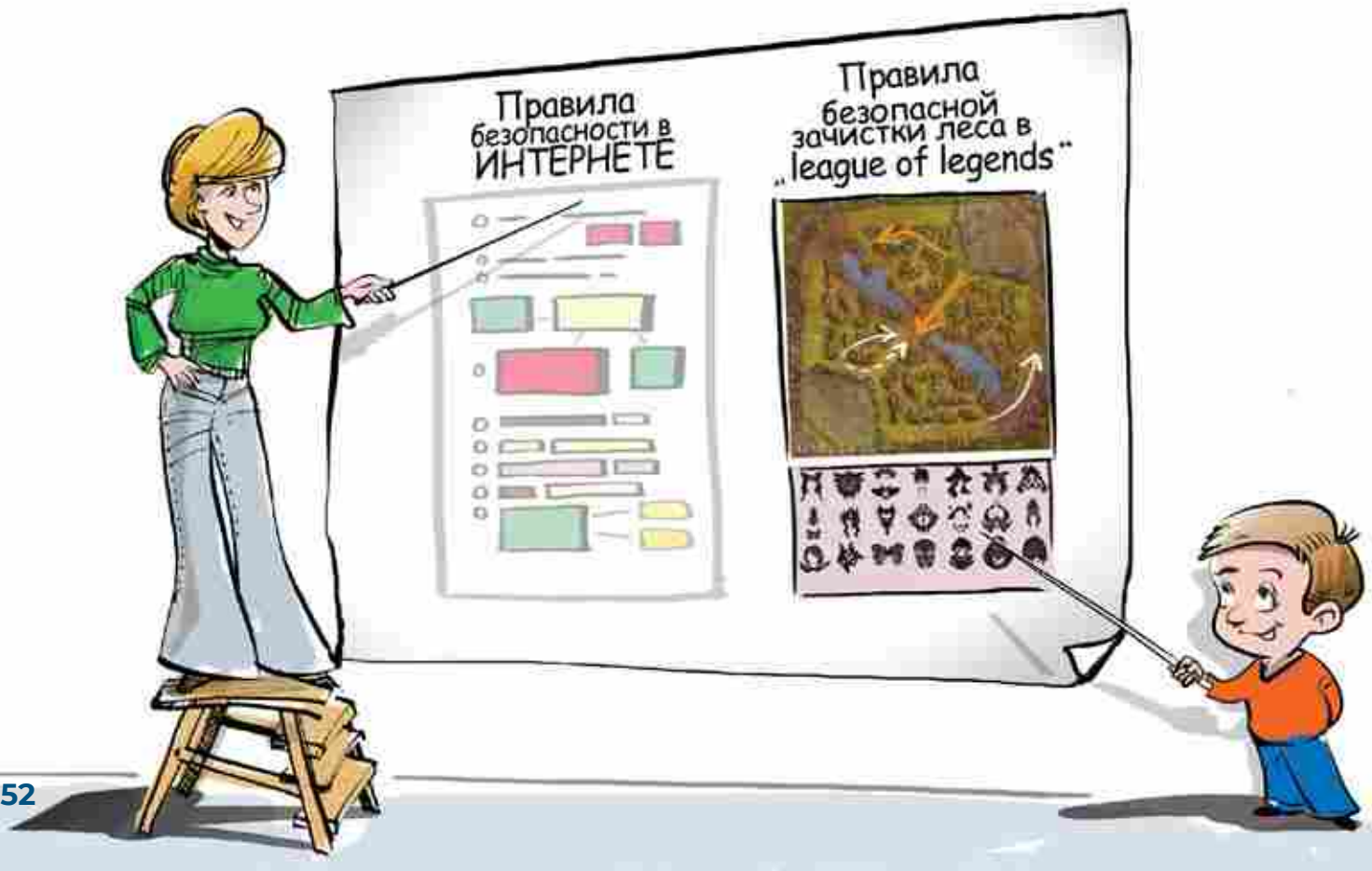
лига безопасного интернета

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



лига безопасного интернета

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ

Телефон горячей линии
8 800 700 56 76

Сайт
найтиребенка.рф
ligainternet.ru

Соцсети
liga
find_child

ligainternet
findchild

Москва, 2023