ГБОУ СОШ №567

# УРОКИ СМАЙЛИКА

2022

*Интерактивное пособие разработано в соответствии с Распоряжением Правительства Санкт-Петербурга № 22-рп от 14.08.2020 "Об утверждении Плана мероприятий по обеспечению информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции в СанктПетербурге на 2021-2027 годы"*

*Рецензенты:*

Журавлева О.Н.,

*Доктор педагогических наук, профессор, проектор по научной работе Санкт-Петербургской академии постдипломного педагогического образования*

*Туманов И.А.,*

*Методист Санкт-Петербургского Центра оценки качества образования и информационных технологий*

Уроки Смайлика. Интерактивное пособие для педагогов, родителей, обучающихся/ Авторы-составители: И.В. Бал, И.А. Битюникова. Под ред. Т.А. Полковниковой, к.п.н., доцента кафедры общественно-научного и культурологического образования СПб АППО 2022. — 77 с.

Электронный образовательный ресурс «Уроки Смайлика» адресован педагогам, родителям (законным представителям) младших школьников, заинтересованным в обучении детей основам информационной безопасности, обучающимся 1-6 классов.

Изучение материалов по информационной безопасности построено как диалог с главным героем – Смайликом. Смайлик позволяет задать позитивный настрой и на практике реализовать принцип «Учение с увлечением!»

«Уроки Смайлика» могут быть использованы как элемент содержания учебных курсов («Окружающий мир», «Информатика»), в организации внеурочной деятельности, для проведения классных часов, бесед, родительских собраний, самостоятельной работы обучающихся, в совместной деятельности детей и родителей.

Электронный образовательный ресурс включает в себя интерактивное пособие «Уроки Смайлика», одноименный сайт и методические рекомендации по использованию ЭОР «Уроки Смайлика»

При создании тестов, викторин, опросов, игр, квестов авторы максимально использовали возможности отечественных цифровых сервисов: Удоба (https://udoba.org/), Interacty https://interacty.me/ru, Etreniki https://etreniki.ru/, Umaigra https://www.umaigra.com/.

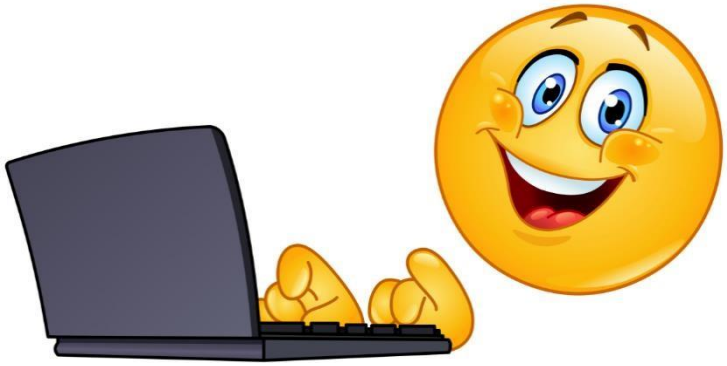
ОЭР «Уроки Смайлика» позволят расширить цифровые компетенции всех участников образовательных отношений и содействовать реализации концепции информационной безопасности детей на практике.

Текст пособия снабжен активными ссылками на интерактивные задания.

## Оглавление

# Дорогой друг!

Тебе предлагается изучить правила безопасного поведения в Интернете. Интернет - это мир компьютерных сетей, где главным является обмен информацией. Чтобы обезопасить от угроз и негативных воздействий себя и свои устройства работы с информацией в Интернете, используй правила безопасного поведения.



Я думаю, вы уже догадались, о чём пойдёт речь на наших занятиях? Конечно, об Интернете. И не просто об Интернете, а об опасностях, которые он в себе таит. Ведь не зря говорят: «Предупрежден – значит вооружен!».

# Давайте знакомиться!

**Привет, Я Смайлик!**

Я живу в электронных сообщениях, в телефоне, почте, Интернете. Смайлик означает “веселый”. Моё имя произошло от английского слова “улыбка” (“смайл”). Меня обычно ставят в конце сообщения, чтобы пожелать добра и хорошего настроения.

Я появился в то время, когда учёные изобрели *компьютерные сети.*

**Кто меня придумал?**

Впервые в истории использовать скобку для обозначения улыбки догадался русский писатель Владимир Владимирович Набоков. В 1969 году в интервью одному из журналов он сказал:

:-)

*“Я часто думаю, что должен существовать специальный типографский знак, обозначающий улыбку, - нечто вроде выгнутой линии лежащие навзничь скобки…”*

В 1982 году американец Скот Фалман предложил использовать двоеточие, дефис и закрывающую скобку для обозначения улыбки. Так появился я, Смайлик. **Прочитай историю происхождения смайлика.**

Теперь меня знает каждый, кто пользуется компьютером или мобильным телефоном. Я расскажу, как вести себя в Интернете, чтобы нести в своих сообщениях добро людям. Ты научишься защищаться от негативных сообщений, от недобрых людей и вредоносных рассылок в сети.

## Задание 1

Попробуй нарисовать смайлик с улыбкой! **Внимательно следуй инструкции.** Этот **видеоурок** поможет тебе создать смайлик в графическом редакторе Paint.

**Задание:** А теперь придумай и нарисуй новые смайлики самостоятельно! Можешь даже нарисовать смайлопортрет своей семьи.

## Задание 2

Попробуй в текстовом редакторе создать краткий словарик смайликов. Понимание значений некоторых смайликов, используемых в электронной переписке, может тебе пригодиться.

**Краткий словарик смайликов**

| Европейские | Значение |
|---|---|
| :-) =) :) | улыбка, радость |
| :-( или =( | грусть, печаль |
| :-D | смех |
| :-C | огорчение |
| :-/ :-\ | сомнение, недовольство или обида |
| :-0 o_O | удивление |
| 8-O =-O | сильное удивление |
| >:-D | злорадный смех |
| }:-> ]:-> | коварство |
| ;-) ;) | подмигивать |
| :-P :-p | показывать язык |

| Азиатские | Значение |
|---|---|
| n_n ^_^ | улыбка, радость, счастье |
| <_> v_v | грусть |
| >_< | злость |
| >_> <_< | сомнение |
| -_-» | стеснительность |
| ^_^» | смущённость |
| *^_^* | сильное смущение |
| -_-# -_-¤ -_-+ | ярость |
| o_o | удивление |
| 0_0 | сильное удивление |
| O_o o_O) | очень сильное удивление |
| @_@ | обалдеть! |
| %_% | глаза устали |

Хочешь пройти шуточный тест и проверить какой ты на самом деле? Выбери любой понравившийся смайлик и переверни страницу.

**Игра**

## Конструктор смайликов

Дизайнер из Сан-Франциско Филипп Энтони запустил веб-сервис Emoji Builder, с помощью которого можно создавать эмотиконы, которых нет ни у кого.

Смайлик можно составить по слоям из нескольких частей: головы, глаз, рта и различных «аксессуаров» (очков, повязок и т. п.) Каждый элемент можно отредактировать: изменить расположение, масштабировать и повернуть под любым углом. В результате могут получаться уникальные эмодзи. Лицо — основной элемент, поэтому оно может быть только одно, а остальные компоненты можно добавлять в любом количестве. Чтобы переместить любую часть смайлика на передний или задний план, достаточно сдвинуть его в правой панели вниз или вверх.

В Emoji Builder также есть кнопка Randomize, которая позволяет быстро генерировать эмотикон из случайных частей. Готовый смайлик можно скачать в формате PNG, а далее отправлять в различных соцсетях и мессенджерах.

😁😊😉😐

**Попробуй создать свой смайлик**

А вот, что получилось у меня

**А хотите поручить создание смайлика искусственному интеллекту?**

Это вполне реальная задача. Сегодня технологии визуализации мышления развиваются стремительно. Приятно, что не отстают и многие наши IT-разработчики. В ноябре 2021 года команда СберБанка объявила о запуске нейросети ruDALL-E, которая способна создавать изображения на основе текстового описания на русском языке. Отмечено: это первая в мире подобная нейронная сеть. Был разработан сервис генерации изображений. За полгода этим сервисом воспользовались 2 млн уникальных пользователей, которые суммарно сгенерировали 125 млн изображений. Суть сервиса заключается в том, что после ввода текста программа обрабатывает ваш запрос и предлагает сгенерированное изображение. Вы можете сгенерировать собственный эмодзи или смайлик. По короткому текстовому описанию ruDALL-E генерирует смайлики, которые можно использовать для стикеров, клипартов и прототипов дизайна. Модель понимает обширный набор понятий и генерирует совершенно новые эмодзи, которых не существовало до этого.


Вот сколько вариантов предложил мне виртуальный художник, когда я вписала "Веселый смайлик". **Попробуйте сами!**

# Моя безопасность и информация в Сети

## Компьютер и информация

**Информация** — это сведения об окружающем мире.

В древние времена люди передавали информацию с помощью изображений: на стенах пещер, на глиняных табличках, на бересте.

Сцены охоты пещера Альтамира

Глиняная табличка

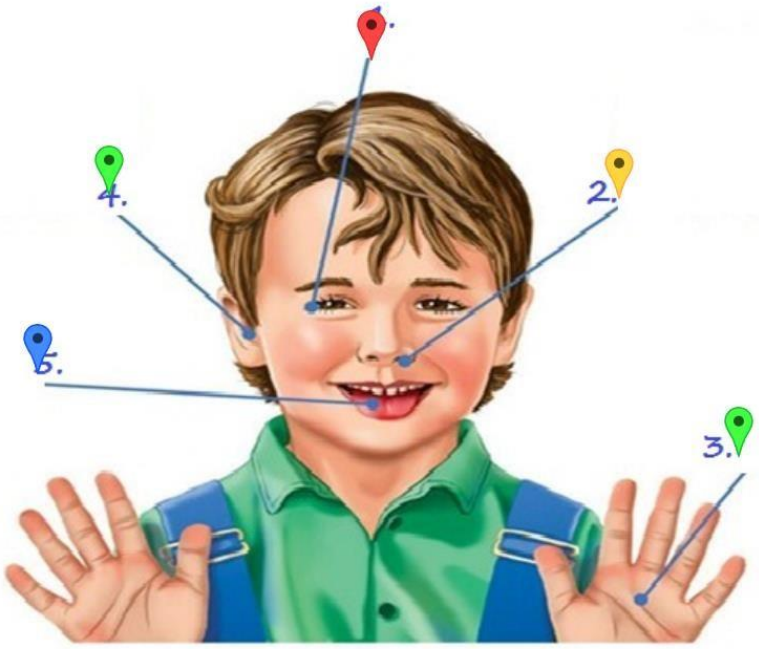
Берестяные грамоты древней Руси

Информацию можно получать разными способами.

Получать информацию нам помогают **органы чувств**. С помощью зрения человек получает зрительную информацию об окружающем мире. Человек видит изображение.

Человек получает звуковую информацию с помощью ушей, слышит различные звуки.

**Задание:** Отметь органы чувств человека.




Выделяют разные **виды информации**.

- **По способу восприятия:**

*Визуальная* - воспринимаемая органами зрения - глазами.

*Звуковая* - воспринимаемая органами слуха - ушами.

*Тактильная* - воспринимаемая человеком с помощью кожи.

*Обонятельная* - воспринимаемая органами обоняния. Носом мы чувствуем запахи.
*Вкусовая* - воспринимаемая органами вкуса. Языком мы чувствуем вкус еды.

- **По форме представления:**

*Текстовая* - передаваемая в виде специальных символов - букв.
*Числовая* - в виде цифр и знаков, обозначающих математические действия.
*Графическая* - в виде изображений, графиков, фотографий.
*Звуковая* - это всё, что можно услышать: музыку, речь человека, шум машин.
*Видеоинформация* - видеозапись.

**Проверь себя!**

**Что такое компьютер? Где он применяется?** В современном мире для хранения, обработки и передачи информации используются различные цифровые устройства, в первую очередь компьютер. Используя компьютеры или смартфоны, мы общаемся друг другом, пишем сообщения, пересылаю фотографии, снимаем видеоролики, чтобы разместить их в Интернете, и делаем многое другое. Несмотря на то, что эти устройства появились сравнительно недавно, они уже прочно вошли в нашу повседневную жизнь, и сейчас достаточно сложно представить себе мир компьютеров, смартфона и Интернета.

**Историю появления компьютера смотри здесь.**
**Проверь себя!**

С помощью компьютера можно создавать, хранить, обрабатывать, передавать на другие цифровые устройства информацию (текстовые сообщения, фотографии, видеофайлы и др.), а также искать информацию. Все эти действия компьютер выполняет по специально составленной компьютерной программе - алгоритму.

**Алгоритм** - это определённая последовательность действий.

В повседневной жизни мы не замечаем, как используем те или иные алгоритмы. Приготовить еду, собраться в школу, перейти дорогу - все эти действия выполняются в определенной последовательности. Человек ежедневно пользуется различными алгоритмами. Например, правила умножения, деления, сложения, вычитания чисел; грамматические правила правописания слов и предложений, а также разнообразные инструкции, рецепты и указания - всё это алгоритмы.

**Сказочный алгоритм**

Наверное, все помнят из детства сказку, в которой рассказывается о местонахождении смерти Кощея Бессмертного: «Смерть моя – на конце иглы, которая в яйце, яйцо – в утке, утка – в зайце, заяц в сундуке сидит, сундук на крепкий замок закрыт и закопан под самым большим дубом на острове Буяне, посреди моряокеяна …».

Предположим, вместо Ивана-царевича бороться с Кощеем был брошен Иван-дурак. Давайте поможем Василисе Премудрой составить такой алгоритм, чтобы даже Ивандурак смог убить Кощея. Расставьте цифры от 1 до 9, чтобы упорядочить действия Ивана-дурака.

| | |
|---|---|
| Из зайца нужно достать утку | |
| Теперь уже можно достать зайца | |
| Поскольку сундук закопан под самым большим дубом, то сначала необходимо найти самый большой дуб на острове | |
| Иголку поломать | |
| Прежде чем доставать зайца, необходимо сломать крепкий замок | |
| Из утки достать яйцо | |
| Разбить яйцо и достать иголку | |
| Затем нужно выкопать сам сундук | |
| Конечно же, сначала необходимо разыскать остров Буян (на такие вещи, будем считать, Иван-дурак способен) | |

Итак, давайте подведем итог.

Подумайте, почему компьютер стал незаменимым помощником человека. 😉

## Интернет

Сегодня мы с вами познакомимся с такими понятиями как **«Интернет», «webстраница», «гиперссылки».**

В современном мире **Интернет** – один из самых популярных информационных систем. С помощью Интернета мы получаем множество возможностей: поиск информации, обучение, игры, общение, просмотр видео и многое другое. Многие путают саму электронную сеть (Internet) с **World Wide Web (WWW),** которая представляет собой взаимосвязанную информационную базу в Internet.

**Информационные системы** – это хранилища большого количества данных на носителях.

**Что такое Интернет?**

**Интернет** — это всемирная сеть, которая состоит из миллионов компьютеров, соединенных между собой.

Интернет предоставляет нам услуги: электронная почта, интерактивное общение, форумы и т. д.



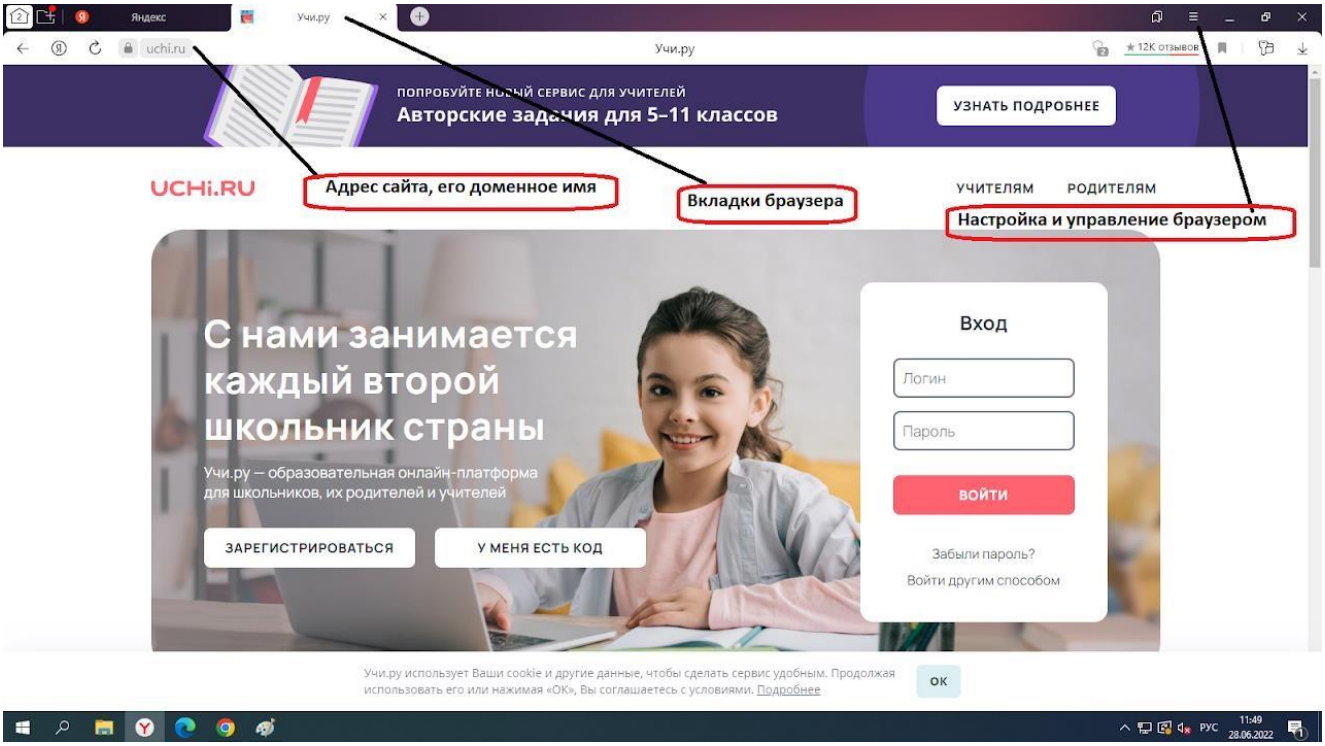
**Сайт –** группа электронных документов в компьютерной Сети. Веб-сайт можно сравнить с книга сайт состоит из веб-связанные содержанию. на его сети времени.

Для просмотра веб-страниц используют специальные программы- **браузеры**, например: Яндекс, Опера, Мозила, Хром и т.д.

**Гиперссылка** – текст, страниц, которые это содержащий ссылки на по смыслу или программа, другие документы. Информация которая используется в страницах доступна любому глобальной для пользователю в любой оформления запроса, момент обработки и просмотра содержания веб-сайтов.

Существует особый способ связи между объектами в сети Интернет – гиперссылка. книгой или журналом. Как и Хром и т.д.

Рассмотри **основные элементы браузера.** 🤔

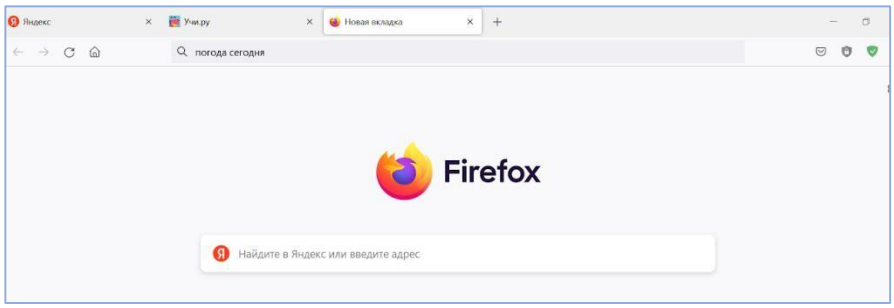



**Доменное имя** — это имя сайта в Интернете. Например, адрес сайта в Интернете может выглядеть следующим образом: **https://uchi.ru**

Так, "учи" - название сайта, а "ru" говорит о том, что сайт находится в российской Сети.

Чтобы открыть очередной сайт, достаточно открыть новую вкладку и переключаться между вкладками по мере надобности.

Также браузер позволяет вводить в адресной строке поисковой запрос. Например: узнать какая сегодня погода.




## Сайты для детей

А ещё Интернет похож на огромную библиотеку! Только вместо книг в интернете есть сайты. Как и книги, сайты бывают разными. Например, есть сайты для игр, чтения, обучения, общения с друзьями.


Кстати, не все сайты в интернете созданы для детей. На детских сайтах есть игры, мультики, интересные задания, а ещё детские песни, рассказы, сказки. Постарайся открывать только детские сайты, потому что там интересно и безопасно!

Я помогу тебе найти безопасное виртуальное пространство. Лучшие сайты для детей собраны на **портале** **«ВебЛандия»**. Но помни, что Интернет — это очень интересное место! Можно так увлечься, что провести в нём весь день. Но это опасно для твоего здоровья! Голова, глаза, шея, спина очень устают и могут заболеть. Проводи в интернете не больше 30 минут в день.

Идея создания **сайта «ВебЛандия. Лучшие сайты для детей»** принадлежит Российской государственной детской библиотеке. К проекту подключились десятки библиотек по всей стране, а также профессиональные психологи, социологи и педагоги. «ВебЛандия» сегодня – это 1695 проверенных сайтов, которые можно использовать для игры, развлечения и обучения. Даже самый пытливый детский ум найдет здесь что-то интересное и полезное для себя. 3D-модели динозавров и познавательные онлайн игры, кулинарные рецепты и лучшие подборки поделок, интерактивные азбуки и полноценный литературоведческий анализ произведений из школьной программы, биографии известных личностей и историю археологических открытий, виртуальные экскурсии по мировым музеям и полезные советы для начинающих предпринимателей.

Для удобства детей и родителей все сайты распределены по 14 разделам.


ВебЛандия предлагает 14 рубрик: ▪

**Животные и растения**

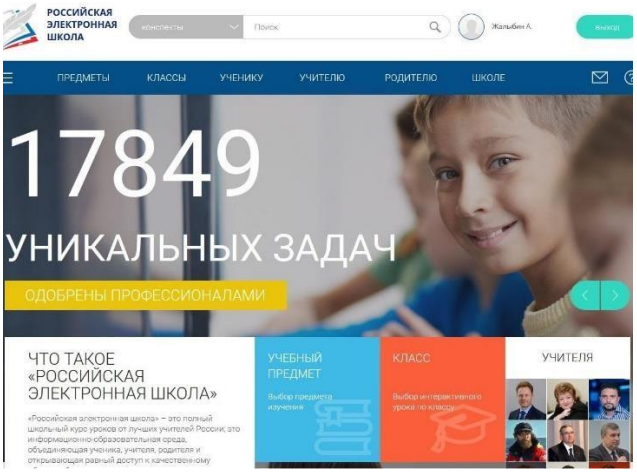
- **Игры и развлечения**
- **Искусство**
- **Литература и лингвистика**
- **История и биографии**
- **Иностранные языки**
- **Математика и естественные науки**
- **Техника и изобретения**
- **Путешествия и туризм**
- **Спорт**
- **Все о человеке**
- **Школьникам и абитуриентам**
- **Электронные справочные ресурсы** ▪ **Экономика, бизнес и коммерция**

## Сайты для учёбы

- **Российская электронная школа**
- **Московская электронная школа**

- **Яндекс. Учебник**
- **Учи.ру**
- **Lingualeo** ▪ **obrazavr**
- **Смарторика** ▪ **Шахматы онлайн**

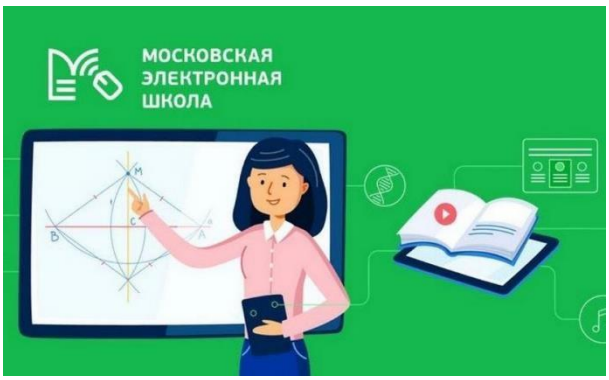
Используй Интернет, чтобы лучше учиться. Развивай свою эрудицию. ищи ответы на вопросы по любому предмету. Какие сайты для учёбы можно посоветовать? Конечно те, которые помогут больше узнать по теме урока, подобрать материал для выступления, а также подготовиться к занятиям в том случае, если ты что-то пропустил.




## Российская электронная школа

Интерактивные уроки по всему школьному курсу с 1 по 11 класс от лучших учителей страны, созданные для того, чтобы у каждого ребёнка была возможность получить бесплатное качественное общее образование.

## Московская электронная школа




В библиотеке МЭШ в открытом доступе находятся более 769 тыс. аудио-, видео- и текстовых файлов, свыше 41 тыс. сценариев уроков, более 1 тыс. учебных пособий и 348 учебников издательств, более 95 тыс. образовательных приложений. С помощью этой платформы можно проверять домашнее задание, общаться с педагогами и находить интересные материалы для подготовки к уроку.


## Яндекс.Учебник

Ресурс содержит более 35 000 заданий разного уровня сложности для учеников 1–5 классов, которые разработаны опытными методистами с учётом федерального гос. стандарта.

## Учи.ру

Крупнейшая российская образовательная онлайн-платформа, на которой более 8 млн учеников со всей страны изучают школьные предметы в интерактивной форме по индивидуальной траектории, учатся программированию, развивают гибкие навыки, готовятся к ВПР и ОГЭ, а также участвуют в российских и международных олимпиадах.

UCHi.RU

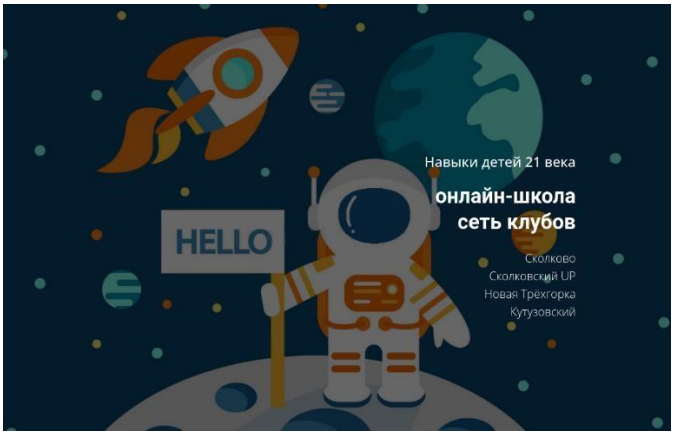

## Lingualeo

Это лучший способ изучать и практиковать языки онлайн:

- здесь ты найдешь более 200 тысяч интерактивных материалов (фильмы, аудио и тексты) от носителей языка;
- создашь личный словарь;
- пройдешь интересные тренировки;
- получишь сертификат по итогам обучающих курсов (грамматика, ЕГЭ и ГИА, бизнес-английский).

## Образавр

Интерактивная онлайн-платформа для изучения школьных предметов на практике с бесплатными уроками и тестами.

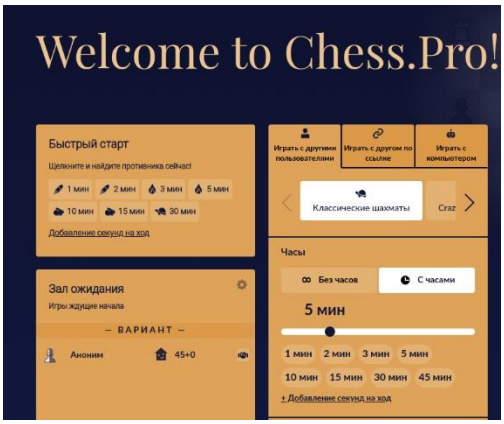



## Смарторика

Бесплатные онлайн-курсы робототехники и программирования роботов для детей от восьми лет.

## Шахматы онлайн

Ресурс, который поможет тебе не только освоить одну из древнейших игр, но и развить стратегическое мышление, умение просчитывать ситуацию на много ходов вперёд, а также эмпатию, стрессоустойчивость и способность держать себя в руках.




**Выполни задание от Смайлика!**

слова: Вместе со своими близкими или учителем найди сайты олимпиад, конкурсов для начальной школы по любимому тобой предмету. Введи в строку поиска *Олимпиады для младших школьников.* Выбери интересный для тебя конкурс

# Фейки в Интернете

Вся ли информация в интернете проверенная и правдивая? Можно ли в интернете встретить ложную информацию? Как её распознать?

В Интернете уже давно известно такое понятие, как **фейковые новости** (ложная информация). С 2016 года количество фейковых новостей и скорость их распространения сильно увеличилась.

**Фейковые новости** - преднамеренное (специальное) распространение ложной информации в Интернете и других средствах массовой информации для того, чтобы ввести в заблуждение читателей.

Основная проблема фейковых новостей заключается в том, что они могут ввести в заблуждение и привести к принятию необдуманного решения.

**Чтобы новости не смогли ввести тебя в заблуждение, Выбирай несколько источников информации и сравнивай тексты сообщений между собой.**

**Занятие 1**

**Фейки в Интернете**

Подсказка для учителя

**Занятие 2**

**Фейкчекинг: как отличить факт от фейка**

Подсказка для учителя

Я расскажу тебе как себя вести, если информация, найденная в Интернете, вызывает сомнение в её достоверности.

| | | | |
|---|---|---|---|
| Не стоит верить одним заголовкам. Заголовок может не соответствовать ее содержанию. | Посмотри информацию об новостиавторе статьи. Попробуй найти его другие публикации. | Используй разные источники информации. | Старайся оценивать информацию объективно. |

**Задание. Вставь пропущенные слова.**

*Спам, пароль, бесплатные робуксы, номер телефона, RuTube*

В _____ часто можно увидеть видеоролики, которые учат получать _____. Обычно это _____, нацеленный на направление молодых людей на веб-сайты, где их просят ввести своё имя пользователя и _____ от компьютерной игры. Вместо бесплатной игровой валюты взламывается аккаунт. Ещё одна афера - просят ввести _____ и побуждают человека присоединиться к платной контентной услуге. Надо быть очень осторожным с любыми обещаниями бесплатных вещей в Интернете.

Проверь себя!

Подумай, верны ли высказывания:

1. В Интернете встречается только проверенная и надёжная информация.
2. Реклама в Интернете может быть встроена в ленту новостей.
3. Фейковые новости могут встретиться в любых средствах массовой информации.
4. Кроме ложных новостей в Интернете можно встретить агрессивную рекламу и непроверенные данные.
5. Непроверенная или ложная информация может навредить.
6. Целевая реклама отражает твои поисковые запросы.

Проверь свои ответы используя QR-код.

Дополнительная информация ☺

**Как обнаружить ложь и остаться правдивым в Интернете**

**Игра «Найди отличия»**

Внимательность - очень важная способность для каждого из нас. Как же везёт людям, у которых она от природы на высоком уровне! Впрочем, тем, кто чувствует, что зачастую важные детали выпадают из его поля зрения, не стоит расстраиваться. Внимательность можно и нужно развивать и найти способы это сделать совершенно не проблема. Ведь на сегодняшний день уже придумано так много увлекательных и красочных онлайн тренажёров - выбирай не хочу!

И один из них - игра "Найди отличия!" **Попробуй сам!**

## Безопасность и онлайн-покупки

В Интернете можно купить практически всё: книги, бытовую технику, компьютерные игры, продукты питания, одежду и многое другое.

Несмотря на большие возможности онлайн-торговли, есть риск, связанный с покупками через Интернет.

**Посмотри видео от Смешариков.** Были ли у тебя похожие ситуации? Как ты поступал в таких случаях?

Всегда и везде нужно соблюдать правила безопасности. Интернет - не исключение. Мышарик преподаст Смешарикам суровый урок, который покажет, насколько они беспечны при заказах товаров из Интернета. Не стоит пользоваться услугами подозрительных сайтов и сообщать свои личные данные неизвестным, и уж тем более ни в коем случае нельзя переводить деньги ненадежным продавцам. Соблюдая эти простые правила, вы сможете защитить себя и свои средства. Будьте внимательны :)

Важно помнить **несколько простых правил** совершения покупок в интернет-магазинах:

1. Попроси взрослых проверить, чтобы все приложения (программное обеспечение) на всех своих устройствах были обновлены до последней версии.
2. Попроси взрослых обновить браузер, которым ты пользуешься для поиска информации в Интернете.
3. Не совершай онлайн-покупки с чужого компьютера, даже если это компьютер твоих друзей или знакомых.
4. Попроси взрослых установить на твоё устройство, компьютер или мобильный телефон, надёжную антивирусную защиту.

### Мошенничество в интернет-магазине

Все большую популярность в России набирает интернет-торговля. Что и не удивительно, ведь торговля через интернет-магазин является удобной и очень выгодной как для продавцов, так и для покупателей.

Продажа товаров посредствам сети интернет весьма привлекательна для предпринимателей.

Во-первых: онлайн торговля не требует наличия «обычной» торговой площадки, достаточно создать виртуальный магазин, который, по сути, представляет собой сайт в интернете.

Во-вторых: у продавца отпадает необходимость в приобретении дорогостоящего торгового оборудования, найме торгового и обслуживающего персонала.

**Плюсы** покупок товаров через интернет-магазин есть и у покупателей. Ведь, зачастую товары, приобретаемые посредством дистанционной торговли, имеют меньшую цену, чем аналогичные товары в стационарной торговой точке. Покупатель имеет возможность не спеша выбрать необходимую вещь, не выходя из дома, тем более что компьютерная техника и интернет сегодня есть практически в каждой семье.

Но, к сожалению, торговля через интернет имеет и свои **минусы** для покупателя.

Покупая в Интернете, можно получить товар, отличный от картинки. А можно вообще ничего не получить, отправив продавцу предоплату.

Потерять свои деньги может и продавец. Известная схема. Появляется покупатель, который "готов" купить товар и внести предоплату. А для этого просит данные карты. После ввода данных исчезает и продавец, и деньги с карты.

**Как безопасно оплачивать товары и услуги в онлайн-магазинах и не потерять свои деньги?**

1. Всегда советуйтесь с родными перед любой покупкой в Интернете, даже в онлайн-игре.
2. Внимательно читайте условия покупки в Интернете.
3. Обязательно познакомьтесь с отзывами покупателей о товаре, который хотите купить.
4. Не переходите по подозрительным ссылкам.
5. Научитесь анализировать рекламу (навязчивая реклама). Низкая цена может быть обманчивой.
6. Совершайте покупки в известных и проверенных интернет-магазинах с хорошими рекомендациями.
7. Учитывайте срок и стоимость доставки.

8. Обратите внимание, что на странице веб-сайта обязательно должна быть представлена информация об адресе (месте нахождения) и полном фирменном наименовании продавца.
9. Обращайте внимание на дизайн сайта. Посмотрите, есть ли признак защиты.

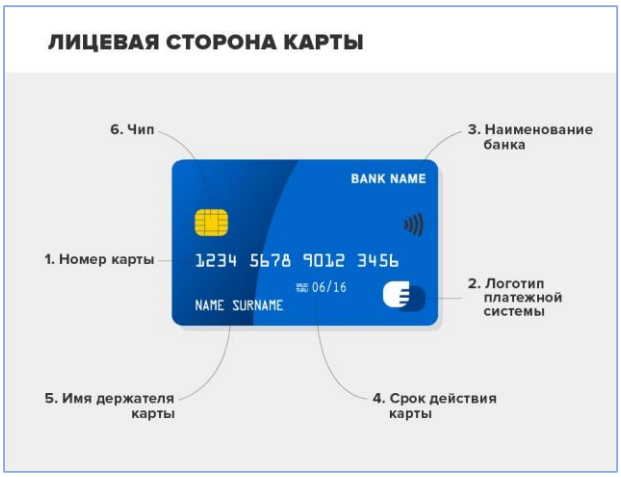
## Банковские карты

### История появления банковских карт

Чаще всего для безналичной оплаты используется банковская карточка. Знаем ли мы, что скрывается за надписями и изображениями на карте?

1. Номер карты.
2. Логотип платежной системы.
3. Название банка, выпустившего карту.
4. Срок действия.
5. Имя держателя карты и владельца счета.
6. Чип.
7. Магнитная полоса.
8. Голограмма платежной системы.
9. Полоса для подписи держателя.
10. Код проверки подлинности карты.
11. Данные банка.
12. Значок бесконтактной оплаты.

**Внимательно рассмотри, какая информация есть на банковской карте.**





**Никому не сообщайте данные своей банковской карты или банковской карты родителей**. Эта информация может использоваться злоумышленниками для кражи денег с этой карты или совершения покупок.

В чем преимущества пластиковых банковских карт перед бумажными деньгами? Чем на самом деле является банковская карта? Как развитие технологий облегчило и ускорило пользование банковскими картами? **Лосяш подробно расскажет обо всем в новой серии новой рубрики!**

Часто ли вы совершаете покупки с помощью сети "Интернет"? А знаете ли вы, как много в интернете мошенников? При покупках через интернет нужно быть очень внимательными, особенно если предоплату требуют сразу и в полном размере, иначе можно легко лишиться своих денег. Чтобы не быть обманутыми, давайте на примере Лосяша узнаем, как себя обезопасить.

**Можно ли оплатить покупку через Интернет? Как правильно это сделать?**

Банки предоставляют услуги интернет-магазинам по оплате товаров и услуг. Перед покупкой любых товаров советуйся со взрослыми. Перед тем как ввести данные платёжной банковской карты, убедись, что не попал на поддельную страницу. После ввода всех данных введи одноразовый пароль, который придёт в виде SMS от банка. Такой пароль никому нельзя сообщать. Процесс покупки немного усложняется и становится более

длительным, зато сильно повышается безопасность покупки через Интернет.

**Задание «Придумай и нарисуй свою банковскую карту»**
**Задание «Безопасный платежи»**

## Разберём ситуации

**Ситуация 1**


Разбор:

Хакеры любят онлайн-игры не меньше, чем дети, но у них на это свои причины. В виртуальном мире бдительность ослабевает, и игроки могут не заметить обмана и клюнуть на уловки мошенников. Например, на предложение «выгодно купить» объекты для игры на фейковом сайте. Игроков заманивают низкими ценами и «уникальными акциями». И не стоит заблуждаться, в подобные ловушки могут попасть не только дети, но и взрослые.

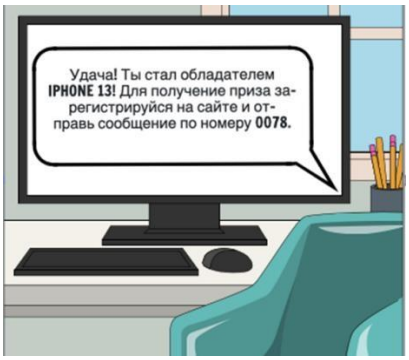
**Прежде чем вводить где бы то ни было персональные данные, пароли, коды или реквизиты банковской карты, удостоверьтесь, что это не мошенническая страница.**

**Ситуация 2**


Разбор:

Если подростку не хватает карманных денег на модный телефон и терпения, чтобы на него накопить, мошенники с радостью ему «помогут». Они размещают в интернете множество объявлений о быстром и легком заработке. Но зачастую в таких случаях внезапно разбогатеть удаётся только самим махинаторам.
Мошенники могут убедить подростка вложить деньги в «сверхприбыльный проект» (спойлер — в финансовую пирамиду). До выплат вкладчикам дело обычно не доходит. Собрав деньги как можно большего числа людей, организаторы исчезают.

**Ситуация 3**




Разбор:

Нередко мошенники рассылают письма и сообщения, в которых обещают нежданный выигрыш, или от имени популярных блогеров запускают рекламу «беспроигрышных лотерей». Но затем за доставку «приза» или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого надо пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь получает убытки.

**Если организаторы конкурса просят что-либо оплатить, это повод насторожиться. Прежде чем пытать удачу в онлайн-розыгрышах, надо убедиться, что организаторы — не мошенники: почитать отзывы в интернете, новости (вдруг они уже замечены в скандалах). Стоит проверить на официальной странице блогера, действительно ли он рекламирует этот конкурс, или он тоже стал жертвой мошенников.**

# Моя безопасность и общение в Интернете

## Что такое "цифровой след"?

**Не хочешь читать - смотри**

Вы когда-нибудь задумывались, сколько информации о вас есть в Интернете? Из ваших аккаунтов, постов, фотографий, комментариев, поисковых запросов и прочих «следов» формируется ваш цифровой образ. Можно сказать, виртуальный двойник. И этот двойник может заинтересовать множество разных людей — причем далеко не всегда безобидных исследователей.

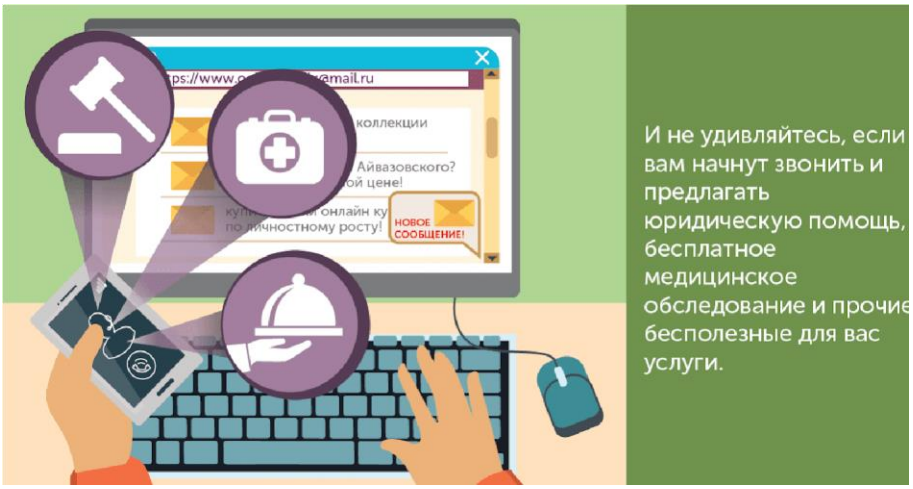
Возьмем социальные сети. Они позволяют вам пользоваться массой удобных сервисов. Формально — бесплатно, но при этом «ВКонтакте» собирают информацию про вас, ваше поведение и предпочтения, чтобы потом продать ее рекламодателям. То же самое делают поисковые системы Google и Yandex.

Возмутительно? Возможно, но имейте в виду: вы сами разрешили им это, когда создавали аккаунт и нажимали на кнопку «Я принимаю…». В условиях соглашений о конфиденциальности, как правило, заранее прописано, что, создавая аккаунт, вы разрешаете собирать информацию о вас и передавать ее посторонним.

Впрочем, иногда примерно то же самое делают безо всякого договора с вами. Продать досье на вас рекламодателям или использовать его в собственных темных целях могут личности, промышляющие тем, что разыскивают и собирают воедино сведения

из открытого доступа — от номера телефона до друзей и групп по интересам в соцсетях.

Оставили контактные данные на сомнительном форуме? Ждите потока ненужных вам писем и назойливых сообщений! И не удивляйтесь, если вам начнут звонить и предлагать юридическую помощь, бесплатное медицинское обследование и прочие бесполезные для вас услуги.




Вы спросили Google, где купить велосипед, — и пару недель баннеры с велосипедами преследовали вас едва ли не на всех сайтах? Это таргетированная реклама. Помимо поисковых запросов, она не брезгует и историей просмотренных веб-страниц — эти данные говорят о круге ваших интересов. Вреда от специально подобранной рекламы нет, но само ощущение того, что за вами следят без вашего согласия, может вызвать чувство дискомфорта.

Решили похвалиться перед друзьями и опубликовали в социальной сети фото билетов на футбол? Кто-то отсканировал напечатанный на них штрихкод и пошел на матч за ваш счет. Это уже не только время и нервы, но и потеря денег. Не говоря уже об испорченных выходных!

Больше всего проблем, пожалуй, ждет тех, у кого в Сеть попали данные паспорта. С их помощью какойнибудь мошенник при должном желании сможет получить на имя невезучего пользователя кредит, оформить липовую фирму или повесить чужие долги.

Информация в сети может храниться очень долго. Резкие посты, написанные по молодости и глупости, могут стать материалом для шантажа лет через 5–10, когда вы добьетесь успеха и будете дорожить своей репутацией. А ваша личная переписка — вообще настоящий клад для желающих обогатиться. Если вашу переписку увидят посторонние, вы поставите под удар не только себя, но и других людей.

Особые возможности дает злоумышленнику сочетание различных данных о вас. Представьте, что он узнал ваш домашний адрес и текущее местонахождение (например, по геотегам на фото). Если расстояние между первым и вторым измеряется в сотнях километров, то к вам домой могут заглянуть непрошеные гости. Тем более что времени на то, чтобы найти все ценное, у них будет достаточно!

## Аватар

**Аватар** — это картинка, которая используется в качестве изображения пользователя в социальных сетях, онлайн играх и форумах. Это может быть как фотография человека, так и просто любое графическое изображение.
**Прочитай об авторе здесь**

Не спеши выкладывать своё фото – выбери картинку, которая покажет твоим друзьям, например, чем ты интересуешься (спортом, домашними питомцами,

рисованием, музыкой…). При выборе аватарки на свою страницу воспользуйся **советами Смешариков.**

Хотите попробовать создать аватарку для своей страницы? Это можно сделать при помощи онлайн сервисов. Переходите по предложенным ссылкам, вас ждет увлекательный процесс. Удачи!

**Аватарка в стиле Майнкрафт**
**Мультяшная аватарка**
**Аватарка в стиле эмодзи**

## Настройки приватности

Персональные данные — это любая информация, которая относится к тебе:

• имя, фамилия
• дата рождения
• номер школы
• номер телефона
• твой адрес и другая личная информация

Персональные данные в интернете нужны для того, чтобы зарегистрироваться на сайте или в социальных сетях, для того чтобы делать покупки или играть в игры. Но, есть данные, которыми мы можем делиться случайно! Задумайся! Это тоже персональные данные, их нужно хранить от незнакомых людей:

- Место нахождения;
- Места учебы;
- Пароли;
- Данные банковских карт родителей;
- Спортивные секции, или другие группы, в которых ты участвуешь.

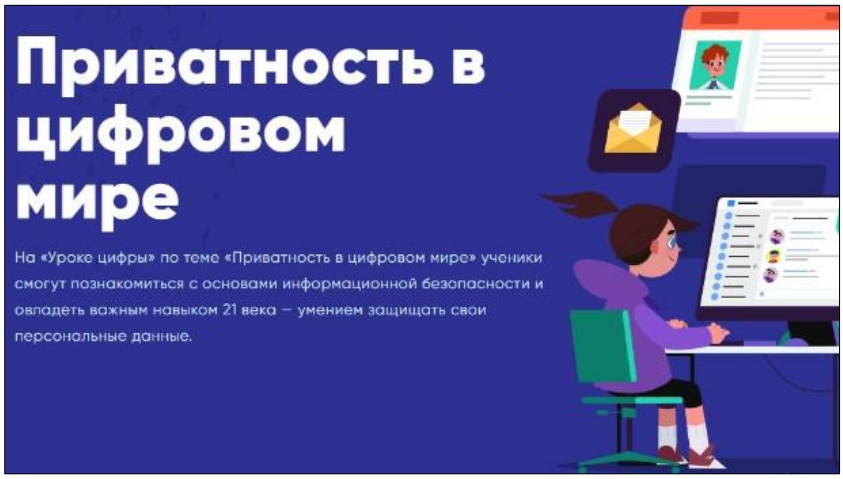
В то же время этими данными могут воспользоваться и злоумышленники. Личная информация, попавшая в сеть, все чаще используется против ее владельцев в форме шантажа, буллинга или мошенничества.

Как обезопасить свои личные данные и свой компьютер от опасностей, которые может таить в себе Интернет? Какие правила нужно соблюдать?

Участвуй во Всероссийском образовательном проекте - **УРОК ЦИФРЫ.** И ты

узнаешь почему важно хранить свои личные данные в секрете, как персональ ная информация попадает в Интернет, что с этими данными могут сделать злоумышленники, как предотвратить утечку и защитить персональную информацию.

На уроке разбираются понятия: «персональные данные», «приватность», «конфиденциальность», «овершеринг», «ци фровой след» и «шпионское ПО». Ты познакомишься с правилами кибербезопасности, которые помогут защитить свои персональные данные.




Полезное видео –

**Как настроить приватность в VK?**

## Надежный пароль

**Не хочешь читать - смотри**

Итак, преступники охотятся за аккаунтами. Они могут получить доступ к учетной записи, если подберут или узнают пароль от нее. Как ее защитить? А как делать НЕ надо?

Начнем с самых частых ошибок в выборе пароля.

Простое слово или короткий набор символов взломщик подберет простым перебором — наугад или по словарю. Аккаунты с паролями вроде 123456, password или love2000 практически беззащитны перед атаками.

Если вы используете в качестве пароля кличку своей собаки, день рождения жены или мужа, то злоумышленник без особых усилий может узнать его из социальной сети. Это плохие пароли!

Но даже хороший пароль может превратиться в плохой, если использовать его для защиты нескольких аккаунтов. Если хоть один сервис окажется недостаточно защищенным и его база данных утечет, то в руках злоумышленников окажется сочетание вашего логина (обычно это адрес электронной почты) и пароля. И преступники решат попробовать эти же сочетания на других сервисах — вдруг подойдет? Если вы использовали один и тот же пароль, то у них получится — и в опасности окажутся сразу все ваши учетные записи.

Наконец, не стоит сообщать ваши пароли кому бы то ни было, даже друзьям. Вы не можете быть абсолютно уверены в их осторожности! Да и возможность ссоры, пусть даже временной, тоже нельзя исключать.

Действительно надежный пароль — во-первых, длинный, как минимум из 10 символов. А для защиты самых важных аккаунтов мы советуем использовать пароль не короче 15 символов.

Во-вторых, надежный пароль — это либо случайный, либо неочевидный для постороннего набор знаков. Он должен включать в себя буквы, цифры и специальные символы. Буквы при этом следует использовать как большие, так и маленькие. Подбор такого пароля может занять годы! У киберпреступника столько времени нет. Постойте, скажете вы, но такой хороший, надежный пароль может стать надежной защитой не только от злодея, но и от хозяина аккаунта. Попробуй запомни 15 случайных букв, цифр и символов! А если его записать на бумажку — кто-нибудь может его найти и узнать

Тут есть маленькая хитрость: пароль должен быть неочевидным посторонним, но вполне может быть логичным для вас. Вы можете, например, взять любую достаточно длинную и известную вам фразу — несколько первых строк из любимой песни, стихотворения или другого текста, который вы уже помните. Составьте пароль из первых букв всех слов, разделенных специальным символом, в конце строк или предложений поставьте цифру — а в начале добавьте первые буквы названия и цвета фона сайта, для которого создаете аккаунт. Это только пример. Вы можете придумать собственную схему и создавать по ней уникальные пароли для каждого аккаунта. А можете воспользоваться генератором паролей. **Генератор паролей**

**К счастью, создать и хорошо защитить надежные пароли несложно.**

1. *Оптимальная длина.* Это элементарный совет, но он работает. Добавь к паролю лишние два-три символа, и этим ты сильно усложнишь потенциальным хакерам жизнь. По данным определённых исследований, лучшим решением будет создавать пароль состоящий не менее, чем из 6–7 символов.

2. *Используйте всё!* Что сюда входит? Пароль должен содержать: Заглавные (A, J, K и т. д.) и мелкие буквы (r, w, g.), цифры и спецсимволы ($, !, & и т.п.)

3. *Задействуйте все области клавиатуры.* Мысленно поделите клавиатуру на 4 части. Спросите себя: “Включает ли мой пароль символы из всех четырёх областей?” В идеале — должен.

**Алгоритмы по созданию сложных паролей**

**Алгоритм 1**

1. Выбираем любое прилагательное. Например, «зажаренный».
2. Выбираем любое существительное. Главное, чтобы это существительное логически не сочеталось с уже выбранным прилагательным. Например, «снежок».

3. Берем цифру, которую легко запомнить (любимую цифру, дату рождения, последние четыре номера мобильного телефона и т. д.). Например, «1984».
4. Берем любой знак препинания. Например, «!».
5. Запишем выбранные слова, цифры и символы в одну строку без пробелов. Получится: «зажаренныйснежок1984!».
6. Поменяем в этой строке какую-нибудь строчную букву на прописную. Например, так: «Зажаренныйснежок1984!». **Алгоритм 2**

Для того чтобы пароль было легче запомнить, сделайте начало, середину или конец всех ваших паролей одинаковым. Например, «I8H!p1n». К этим символам добавьте части, которые ассоциируются с конкретным сервисом, для которого этот пароль предназначен, например для почты — «mail». В результате получим: «I8H!p1nmail».

**Алгоритм 3**

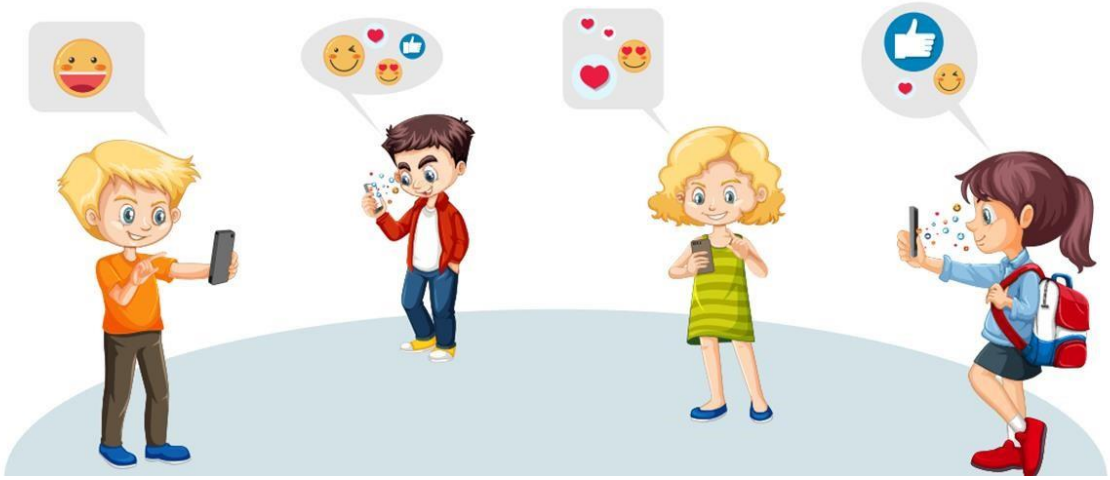
В качестве пароля можно использовать словосочетание, которое известно только вам и имеет отношение к соответствующему сайту. Например, выбирая пароль для электронной почты, вы можете составить такую фразу: «Мой друг Вася 1 раз в день присылает мне смешные письма». Затем нужно ее транслитерировать и взять первую букву каждого слова. В результате получится: «MdV1rvdpmsp». Угадать такую комбинацию невозможно. Поступайте так же, когда выбираете пароли для других сайтов.

Предлагаем вашему вниманию сервис **Проверьте свой пароль.**

При помощи данного ресурса вы можете проверить надежность паролей в своих аккаунтах.

# Публикация информации в социальной сети

**Социальные сети** – это интернет-сервисы, предназначенные для общения, поиска друзей, объединения в группы по интересам и свободного времяпрепровождения. На сегодняшний день это самые популярные площадки для общения, публикации различной информации и её поиска. Популярность социальные сети приобрели изза простоты использования и разнообразных возможностей, которые они могут предложить.



По участвуй в социологическом исследовании по теме: «Социальные сети в жизни школьников».

**Ответь на вопросы смайл-анкеты.**

Но, прежде чем выложить какую-то личную информацию в сети, подумай, не может ли она быть использована против тебя. Не содержатся ли в ней факты, над которыми могут посмеяться другие? Больше советов о том, что можно публиковать в социальной сети ты получишь, если посмотришь **видео на этой странице.**

Проверь себя! выполни упражнение. 😉 **Впишите слова в правильные поля**

*Домашний адрес, файлы, псевдонимом, фотографии, пароль, имя, спам.*

Не разглашайте личные данные. При регистрации старайтесь не называть_____ , фамилию, возраст,_____, номер телефона. Выбирайте такой_____, о котором никто не сможет догадаться. Подумайте, прежде чем что-либо размещать в интернете:_____, видео и др., что они могут стать

общедоступными и быть использованы против вас. Не нарушайте e-mail-этикет. При личной переписке пользуйтесь постоянным онлайновым именем или подписывайте им все письма. Не рассылайте ненужную информацию, большие . Никогда не открывайте и не пересылайте нежелательные электронные письма ( ).

**Давайте поиграем!** 😁

## Электронная почта

Современный мир без электронной почты представить уже невозможно. Сотни миллионов почтовых ящиков, триллионы сообщений ежегодно, терабайты данных ежедневно. Адрес электронной почты стал для современного общения столь же обязательным, как домашний адрес и номер телефона.

Электронная почта уже стала неотъемлемым средством делового и личного общения.

**Рэй Томлинсон** официально признан разработчиком электронной почты для интернета. Созданная им программа в 1971 году позволяла обмениваться почтой между разными компьютерами.

Для работы с электронной почтой используется электронный ящик. У каждого пользователя свой адрес почтового ящика. Каждый электронный адрес состоит из двух частей, отделённых между собой значком @. Этот знак называется «амперсанд», в разговорной речи «собака».

Так выглядит адрес электронной почты:

**Имя_пользователя@адрес_почтового_сервера**

Левая часть указывает на владельца почтового ящика, а правая часть содержит адрес почтового сервера.

В качестве имени почтового ящика можно выбрать любое название, свое имя, фамилию. Имя почтового ящика дает первое представление о человеке. Поэтому следует подумать, не будет ли нелепо выглядеть слишком оригинальное название почтового ящика.

Имя сервера – это адрес службы, которая выделяет пользователю пространство для его почтового ящика. Имя сервера указывается после знака @ («ат»).

В русском языке знак @ принято называть собакой. Есть предположение, что это название появилось благодаря одной из первых компьютерных игр, главного

героя сопровождал песик, который обозначался этим символом. В других странах значок @ называют по-разному: обезьяной, лягушкой, улиткой, свиным хвостиком, хоботом слона.

Существует множество разных почтовых серверов:

@mail.ru @yandex.ru

@gmail.com и др.

Служба доставки электронных писем также может называться е-мейл или интернетпочта. В русском языке принято говорить «электронная почта», а для указания адреса писать по-английски «email».

Электронное письмо можно отформатировать, добавить к тексту изображения, смайлики, а также прикрепить документы, созданные в различных редакторах.

Возможность обмениваться электронными письмами возникла задолго до появления «всемирной паутины», и долгое время электронная почта была главной услугой первых компьютерных сетей. Очередной **выпуск программы "Почемучка"** посвящен тому, как работает электронная почта.

**Задание. Найди слова по теме "Электронная почта"**

| Э | Ъ | Я | Ю | К | К | Ь | И | И | Ё | У | А | Ч |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| К | Й | Щ | Ж | Б | Р | А | М | Ш | Ъ | Ц | А | Ш |
| Ж | Я | И | С | Х | О | Д | Я | Щ | И | И | Ж | В |
| С | З | К | Н | К | Т | Э | Т | Э | Б | Д | А | Р |
| Й | З | П | Э | С | П | А | М | Ю | Ъ | Ы | Ф | Ш |
| Л | В | Ф | Т | Л | Р | М | Ф | У | Ю | Ю | Д | Э |
| Щ | Ы | Т | Е | М | А | Й | Ж | Ш | О | П | Ы | Д |
| М | М | Е | Ч | П | В | Х | О | Д | Я | Щ | И | И |
| Х | Р | М | Ш | Щ | Л | И | Е | Ь | Ц | Ы | Ъ | И |
| К | Ф | Д | Ч | Ы | Е | Я | Ё | Ь | Д | Т | Ч | Д |
| К | О | Р | З | И | Н | А | Л | Ф | О | Ъ | В | А |
| Й | Ы | Я | Р | Ц | Н | К | Э | Ю | Г | Х | Ё | Ф |
| Я | Д | С | Ф | Ь | Ы | Ч | Ъ | З | Н | Ь | Ц | Н |
| О | В | Й | Е | З | Е | М | Ь | Ж | Ш | Ф | Ё | И |

1. Отправленные
2. Исходящии
3. Корзина
4. Имя
5. Спам
6. Ящик
7. Входящий
8. Тема

**Помни о правилах этикета при общении по электронной почте!** ☺

**Презентация о правилах этикета при общении по электронной почте**

А теперь можно и поиграть. Приглашаю вас в заколдованный замок 🙃🙃🙃. **Необходимо расколдовать замок, решая головоломки старой ведьмы.**

## Как безопасно пользоваться электронной почтой

В современном мире, где технический прогресс движется вперед не по дням, а по часам, трудно найти человека, у которого нет электронной почты. Трудно, но не невозможно. Таким оказался и наш Копатыч. Первое, что нужно сделать, когда заводишь новый электронный ящик - придумать к нему пароль. Однако, если пароль будет слишком простым - злоумышленники легко взломают его. **Послушает ли Копатыч программу Ваш Лосяш и придумает сложный пароль, или же под угрозой окажутся все Смешарики?**

При работе с электронной почтой соблюдай эти правила:

● Не каждое письмо нужно открывать, не каждое вложение – скачивать.

Письма могут отправлять злоумышленники, а во вложениях могут находиться вредоносные программы, которые запускаются после того, как их скачают и откроют. В большинстве случаев злоумышленников интересуют деньги или персональная информация (например, паспортные данные). Некоторые вирусы создаются просто для развлечения – вот только компьютеру, на который они попадают, становится не до веселья.

● Не все ссылки в письмах безопасны.

Нужно быть очень внимательным при переходе по ссылкам из писем, ведь некоторые из них хорошо маскируются и ведут на сайты, очень похожие на известные ресурсы, интернет-магазины или магазины приложений и так далее. Если переходить по таким ссылкам, а затем регистрироваться на фейковых сайтах, злоумышленники могут воспользоваться сведениями, которые потребовалось указать при регистрации.

● Не все владельцы почтовых ящиков указывают настоящие сведения о себе.

Интернет дарит людям анонимность: можно назваться кем захочешь, писать что угодно, в том числе оскорбления и ложь. Не стоит верить незнакомцам, от которых приходят письма, и уж точно нельзя сообщать личные сведения о себе и своей семье.

**Задание. Найдите все слова**

| Н | Р | И | И | Б | П | У | Н | Т | Х | Ф | Л | К | Щ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ф | Ч | Л | Р | Е | Г | И | С | Т | Р | А | Ц | И | Я |
| К | И | С | Ф | З | З | П | И | Ц | Ё | К | И | П | О |
| Ё | П | Х | П | О | Ч | Т | А | Ы | К | Ъ | Э | З | В |
| М | Л | К | С | П | Й | Ю | Щ | Б | Ъ | Э | С | Ъ | М |
| П | Ф | Т | П | А | Р | О | Л | Ь | С | Н | Ж | Ч | Т |
| Ж | Ъ | З | Ю | С | П | А | М | В | Ш | З | Ё | Р | Ш |
| О | Б | Щ | Е | Н | И | Е | Л | Ь | Е | Й | Т | Ю | К |
| Ю | Н | Э | Ъ | О | В | Х | Э | В | Э | Ъ | Ш | Ш | П |
| В | И | Р | У | С | И | Ь | Ц | Ь | Р | У | Ь | Н | Ш |
| М | Я | М | Э | Т | И | К | Е | Т | Т | Ъ | Ф | Л | В |
| Ф | З | Ш | А | Ь | О | Б | Э | И | В | Ч | Ш | Л | Т |

1. **БЕЗОПАСНОСТЬ**
2. **СПАМ**
3. **РЕГИСТРАЦИЯ**
4. **ОБЩЕНИЕ**
5. **ПАРОЛЬ**
6. **ВИРУС**
7. **ЭТИКЕТ**
8. **ПОЧТА**

## Фишинг

Фишинг — это рассылка фальшивых писем от якобы надёжного источника.

Например, вам приходит сообщение с требованием восстановить пароль от личного кабинета электронной почты и банковского приложения. Отправитель, на первый взгляд, надёжный, но при внимательном изучении оказывается, что имя и название просто очень похожи на оригинал. Целью таких писем является получение конфиденциальных данных. Например, номеров и пин-кодов к банковским картам или паролей к различным аккаунтам.

Когда ты получаешь сообщение в Интернете, обращай внимание на те, которые содержат:

- угрозы твоему здоровью и благополучию;
- угрозу заражения компьютера вирусом;
- сообщения о выигрыше денежного приза или дорогого подарка в розыгрыше, в котором ты не участвовал. Особенностью такого сообщения является то, что от тебя потребуются минимальные усилия (внесение денежных

средств, которые будут незначительными по сравнению с суммой выигрыша), или наличие других претендентов на это приз;

- обращение по имени, информацию о том, что ты посещал кинотеатр или был в отпуске со взрослыми. Эти сообщения выглядят так, будто составлены специально для тебя.
- просьбу совершить действие (оплатить что-либо или перейти по ссылке на мошеннический сайт, оставить отзыв или комментарий) в короткий промежуток времени. Такие ограничения стимулируют пользователя совершить необдуманный поступок.

К любому сообщению стоит относиться критично. НЕ спеши оставлять свои данные незнакомым людям или вводить их в специальную форму на сайте.

## Кибербуллинг

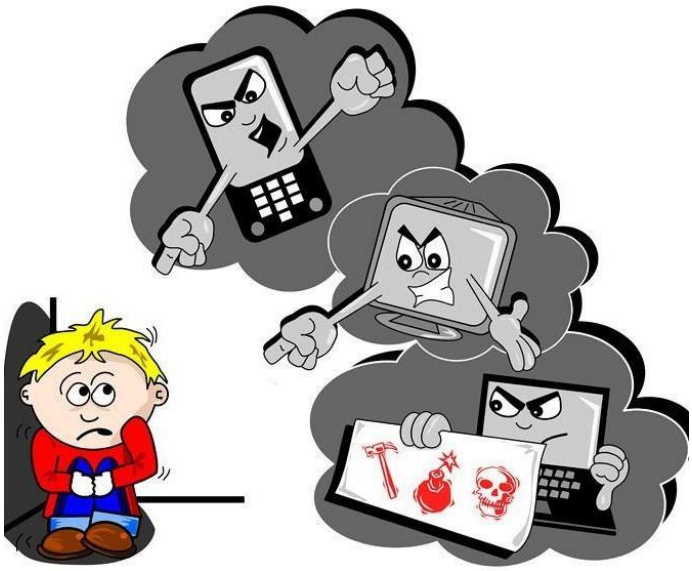
**Кибербуллинг, троллинг, моббинг** — еще недавно никто не знал этих слов, а сегодня травля в Интернете стала предметом беспокойства на государственном уровне.

**Что случилось?**

С появлением Интернета травля часто происходит в социальных сетях, на форумах, в письмах, в мессенджерах, в чатах в онлайниграх и так далее. В последние несколько лет часто используют специальный термин — кибербуллинг. И есть еще несколько терминов, описывающих конкретные виды буллинга, — троллинг, аутинг и другие.

**Как происходит травля в интернете?**

По-разному. Иногда создают специальные страницы, посвященные издевательствам над каким-то конкретным человеком (например, однокурсником или одноклассником). Там размещают издевательские карикатуры, публикуют унизительные фотографии или видео, придумывают обидные прозвища, распространяют о жертвах унизительные слухи.



Иногда людей заваливают комментариями или личными сообщениями с оскорблениями и угрозами. Еще один популярный способ травли — публикация сведений о жертве вопреки ее воле (иногда при этом человека шантажируют). Бывает, что люди пишут от лица жертвы сообщения ее близким, коллегам или преподавателям — это тоже распространенный способ издевательства.

**Как избежать кибербуллинга?**

Во-первых, есть множество разных технических решений. Фейсбук, «ВКонтакте» и другие социальные сети позволяют избавиться от неприятных комментариев и сообщений **с помощью настроек**. Вы также можете запретить людям отмечать себя в записях и на фотографиях. В конце концов, обидчиков можно просто заблокировать.


Кроме того, если кто-то оскорбляет вас в социальной сети, на него можно пожаловаться администрации ресурса с помощью кнопки «Report» («Пожаловаться»).

Еще есть вариант помощи. к которому можно прибегнуть. В нашей стране работает горячая линия "Дети онлайн". На неё можно обратиться бесплатно по телефону с 9.00 до 18.00 по московскому времени или при помощи электронной почты.

Телефон горячей линии: 8-800-25-000-15

Адрес электронной почты: **helpline@detionline.com**

А вы знали, что 11 ноября — день борьбы с кибербуллингом?

**Кибербуллинг** — это травля в сети, когда волна агрессии от многих людей направляется на одного человека или компанию. И это правда страшно!

Давайте остановим травлю вместе! Поддержите эту акцию в своих социальных сетях, используя хэштег **#неткибербуллингу** И пусть этот символ любви и поддержки поможет победить ненависть в интернете! Узнать все о кибербуллинге можно здесь **kiberbulling.net**

Непросто принять верное решение, попав в сложную ситуацию впервые. Если столкнулся с травлей в интернете, в этом **видео** ты найдешь советы, как реагировать, и научишься справляться с кибербуллингом.

Предлагаю сыграть тебе в **игру "Крестики-нолики. Кибербуллинг".** Правила тебе известны. Только прежде, чем поставить значок в клетку, тебе нужно будет ответить на вопрос. Попробуем?

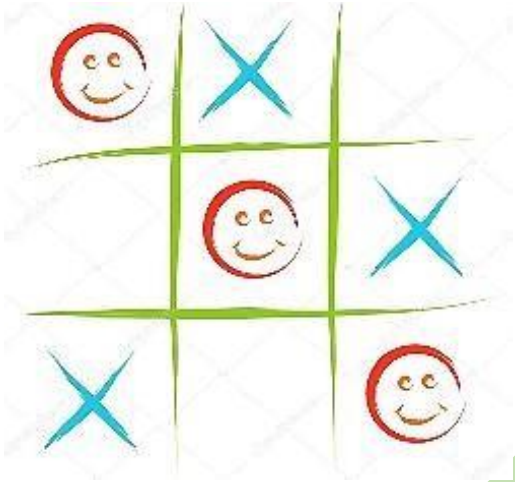
*Дополнительная информация для учителя*

1. Воркбук по антибуллингу для детей и подростков **«Как защититься от травли в интернете и самим не стать хейтерами».**

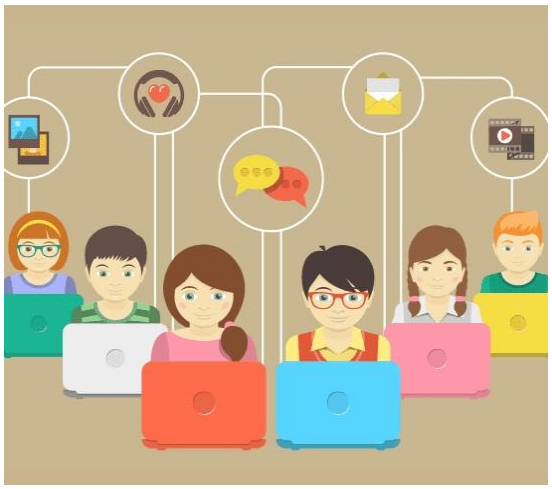
Скачать разворотную версию для печати можно **по ссылке**.

Воркбук поможет разобраться в том, что такое кибербуллинг. На конкретных примерах, а также с помощью наводящих вопросов, творческих и практических заданий дети и подростки узнают эффективные инструменты по предотвращению и прекращению травли в интернете для любой из ролей: жертвы, хейтера или свидетеля.

2. Карта добрососедства: учимся противостоять агрессии в интернете **ссылка**
3. Плакат для профилактики кибербуллинга **ссылка**
4. **Классные игры.рф**



# Детские социальные сети



**Социальная сеть** — это интернет-сервисы, предназначенные для общения, поиска друзей, объединения в группы по интересам и свободного времяпрепровождения.

Контент в соцсетях создается непосредственно самими пользователями. Контент — это содержимое веб-страниц, соцсетей, каналов в мессенджерах и разных программ.

В соцсетях можно публиковать различную информацию: фотографии, видео, текстовые записи, музыку. Можно выражать реакцию на свои и чужие публикации (комментарии, "лайки" и возможность поделиться записью). Можно общаться с помощью голосовых, текстовых сообщений или видео сообщений с другими пользователями социальной сети.

**Детские социальные сети**


## Социальная сеть «Смешарики»

Медиа структура была разработана на основе одноименного детского мультсериала. На платформе у детей есть возможность участвовать в разнообразных игровых турнирах, слушать сказки и общаться с друзьями. Если у ребенка возникают какие-либо вопросы, то на помощь всегда придут знакомые герои мультика.

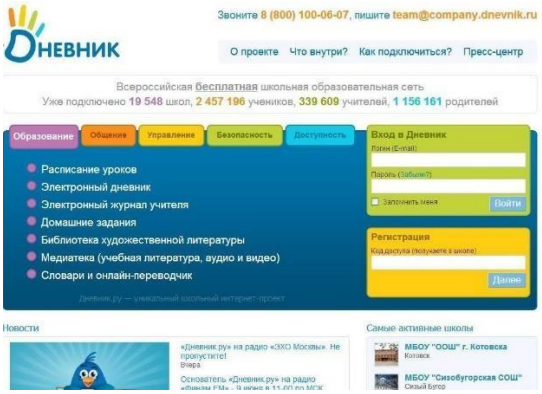
Социальная сеть для детей разработана таким образом, что родители тоже могут найти в ней полезную информацию о воспитании. Также есть рейтинг самых активных пользователей и форум для общения.


## Развлекательный интернетпортал для детей "Миры Твиди"

tweegee.ru - Социальная сеть для подростков и детей. В нашем проекте присутствуют виртуальные миры твиди.

В этих мирах пользователь управляет своим персонажем ("кругликом"), общается с другими пользователями, играет в многопользовательские онлайн игры, в которых можно зарабатывать виртуальную валюту - твидики.

Твидики можно тратить в различных магазинах, приобретая различные вещи и товары необходимые для жизни круглика. Замечатки - новости нашего проекта, иногда в них появляются новости, которые не публикуем в группе вк**,** поэтому важно следить за ними, вдруг мы там разыгрываем твидики? ;)




## Социальная сеть «Дневник.ру»

Этот медиа проект был разработан как для школьников, так и для педагогов. В «Дневник.ру» есть несколько разделов. Они касаются не только школы, но и всей общественной жизни школьника. Там можно отслеживать результаты ГТО, контролировать школьное питание и дополнительные развивающие кружки, и занятия.

Также в социальной сети можно отслеживать рейтинг всех учеников конкретной школы, и своевременно получать всю важную и необходимую информацию.


## LEGO® Life

LEGO® Life — безопасная социальная сеть, разработанная специально для детей. Ребенок может найти друзей и пообщаться с другими детьми, используя смайлики и комментарии в бесплатной соцсети, обеспечивающей полную безопасность ребенка в цифровой среде. Дети могут создать аватар, подчерпнуть вдохновение из видео со сборкой и поделиться своими постройками LEGO с друзьями в модерируемом сообществе. Идеи для строительства, возможности для общения и поиска друзей, анимация и увлекательные детские конкурсы по конструированию делают социальную сеть LEGO Life идеальной платформой для детей. Уникальное приложение LEGO для общения онлайн с друзьями развивается с помощью детского воображения.

Фиксики разбираются во всем и, конечно, в том, как устроен Интернет. В сети очень много полезной информации, но таятся в ней и опасности. Как их избежать? **Фиксики расскажут!**

Антивирусная компания ESET провела международное исследования первых шагов детей в Интернете. Как оказалось среди опрошенных российских детей 61% зарегистрировались в социальных сетях еще до 11 лет. Причем 24% впервые зарегистрировались в семь лет, а 16% — в восемь лет.
Отметим, что это было проделано несмотря на официальные возрастные ограничения в большинстве социальных сетях.

Также 66% опрошенных детей до 11 лет самостоятельно устанавливают приложения на смартфоны. При этом 26% пользуются магазинами приложений с восьми лет, 12% — с десяти лет и 13% — с десяти лет. Об этом сообщает "Рамблер".
Поэтому, если ты уже зарегистрирован в соцсетях, или собираешься это сделать в ближайшее время, внимательно изучи информацию на этой странице.

**Домашнее задание:** Перейди по **ссылке** и выполни задания на рабочем листе.

## Моя безопасность и гаджеты

# Компьютерные вирусы

В мультфильмах и на картинках компьютерные вирусы изображают как фантастические и недружелюбные существа с длинными лапами или щупальцами, при этом чаще всего выбирая фиолетовый или тёмно-зелёный цвет.

На самом деле это не так. **Компьютерный вирус** — это вредоносная компьютерная программа. Общим признаком такого типа программ считается возможность совершать на компьютере или смартфоне пользователя разные действия без участия самого пользователя.

Вредоносные программы принято разделять на следующие группы:

1. **Вирус.** Может выполнять множество различных операций, заражает другие файлы.
2. **Червь.** Устанавливается на устройстве пользователя и ищет способы дальнейшего распространения по сети.
3. **Троян.** Загружается пользователем под видом приложения, однако вместо заявленного функционала троян делает то, что нужно злоумышленникам.

Чем опасен вредоносный код?

- Технически вредоносный код может:
- получать доступ к логинам и паролям от различных сервисов;
- изменять файлы, делать копии и шифровать их;
- получать доступ к данным пользователя (фотографиям, документам, видео и другим данным), а также к данным, которые используют установленные на устройстве программы.

Всё это может навредить пользователю.

**Как распространяются вирусные программы?**

Чаще всего они попадают на компьютер пользователя через вложение (прикреплённый файл) к электронному письму или сообщению в мессенджере. В таких сообщениях мошенники убедительно просят установить программу на свой компьютер или другое техническое устройство. Распознать вредоносную программу можно по расширению, которое имеет прикреплённый к сообщению файл.

Еще одним вариантов попадания вредоносного кода на компьютер пользователя является переход по ссылке на специально созданный веб-сайт. Такой переход может повлечь за собой начало загрузки вредоносной программы.

**Как обезопасить свой компьютер от вируса?**

1. Никогда не открывай вложения, присланные из непроверенных и незнакомых источников.
2. Обязательно проверь флеш-накопитель (флешку) или любой другой носитель информации перед использованием на своём компьютере и после использования на чужом компьютере при помощи антивирусной программы.

**Проверь себя!**

Выбери правильный ответ (может быть несколько).

1. Компьютер исправен, если...

- Программы работают медленно
- Компьютер работает с обычной скоростью

2. В компьютере, возможно, что-то вышло из строя, если…

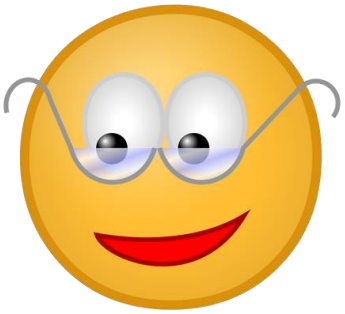
- Программы открываются сами по себе

- Программа все время вылетают

- Файлы не открываются

3. В компьютере, очевидно, есть вирус, если…

- Курсор мышки не двигается
- На Рабочем столе добавляются иконки
- Стартовая страница Web-браузера самопроизвольно изменилась - Компьютер сам перезагружается
- Компьютер больше не работает
- Антивирусная программа в компьютере сообщает, что обнаружен вирус



## Программы для защиты компьютера

Как защитить свой компьютер и другие цифровые устройства от вредоносных программ?

Любой пользователь знает: чтобы надёжно защитить свой компьютер, необходимо не только знать об угрозах и соблюдать базовые правила безопасности в Интернете, но и использовать специальные программы - антивирусы. Чтобы обезопасить свою работу, нужно использовать антивирусные программы.

**Антивирусная программа** — это программа, которая защищает устройство от действий вредоносных программ.

А у вас есть антивирусная программа? Как нет? Знаете, **что случилось с Дим Димычем, когда он нажал на незнакомую яркую картинку**? Хорошо еще, что фиксики были рядом!

Антивирусных программ много, и все они отличаются друг от друга. Вот некоторые характеристики таких программ с точки зрения пользователя:

1. **Платный или бесплатный продукт.**

Есть такие антивирусы, которые:

- являются бесплатными, но дополнительные функции в них включаются за деньги;

- имеют бесплатный пробный период, а затем необходимо приобретать полную версию.

Чаще всего антивирусные продукты продаются с лицензией сроком на один или два года.

**2. Детектирование программ.**

Поиск и обнаружение вредоносных программ, которые антивирус может определить (обнаружить).

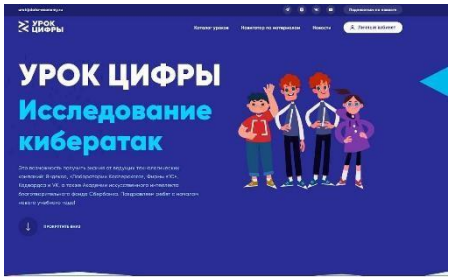
**3. Разнообразие функций.**

Есть антивирусы, которые умеют работать только с вредоносными программами, а есть и такие, которые включают в себя и модуль борьбы с фишингом и спамом.

Важно помнить и о том, что необходимо регулярно обновлять свою операционную систему на домашних компьютерах, смартфонах и планшетах.

**И снова приглашаю тебя поучаствовать в Уроке Цифры!**

«Урок цифры» предлагает погрузиться в увлекательную визуальную новеллу-комикс, сюжет которой строится вокруг исследования кибератаки, совершенной на банк. Сюжет истории основан на **реальных событиях**, которые происходили в разных странах мира!




**Ну а теперь можно и в футбол поиграть!**

## Мобильный телефон

Мобильным телефоном пользуются для разговора на расстоянии и для передачи текстовых сообщений. Сейчас это самый распространённый способ общения среди людей. Главное достоинство мобильного телефона в том, что его можно носить с собой и в любом месте быть постоянно на связи.

Современные телефоны (их называют смартфоны, то есть умные телефоны) подключаются к Интернету. Поэтому с помощью смартфона можно использовать различные возможности этой глобальной сети.

В мире миллионы мобильных телефонов, люди связываются друг с другом по нескольку раз в день.

Они могут разговаривать, даже видеть своего собеседника на экране, посылать текстовые сообщения через **SMS - службу мгновенных сообщений**, контактировать по сетям рассылок, передавать картинки, видео- и звуковые записи.

Нужно соблюдать культуру общения, а также осторожность при получении звонков и сообщений от незнакомых тебе адресатов. О некоторых "телефонных опасностях " можно прочитать **здесь**.

## Телефонные опасности

**1. Телефонные хулиганы.**

Если домашний телефон подвергся атаке телефонных хулиганов, не надо вступать с ними в пререкания и ругаться — ведь это и является их целью. Необходимо сразу обратиться в полицию.

**2. Телефонные мошенники.**

Никогда не стоит поддаваться на провокации! Нужно трезво оценить обстановку и не поддаваться панике, перезвонить родным, обратиться в полицию. Не стоит давать свой номер чужим людям.

**3. Телефонные «прилипалы».**

Не стоит подключать различные приложения, услуги, отправлять смс на предложенные «прилипалами» номера. Если вы оказались в роуминге, вести дорогие междугородние переговоры можно только в случае крайней необходимости, а отвечая на входящие звонки помнить, что это может вам обойтись очень дорого!

**4. Телефонные «террористы».**

Необходимо помнить, что существует административная и уголовная ответственность за заведомо ложные сообщения о пожаре, угрозе террористического акта и другие социально-опасные сообщения.

**5. Осторожно, телефон!**

Сотовый телефон сам представляет собой источник опасности.

-может взорваться при неправильном обращении, например, при перегреве.

-может использоваться террористами как футляр для взрывчатки.

-может привести к помехам в радиосвязи и создать угрозу для пилотирования воздушных судов.

**6. Когда тайное становится явным.**

Когда бы вы ни говорили, вас обязательно слышит кто-то еще, не говоря уж о телефонных прослушках. Поэтому если вам срочно необходимо сообщить что-то «не для общих ушей», постарайтесь найти максимально удаленное место. А для особо важной и секретной информации телефон вообще лучше не использовать.

**7. Телефонная зависимость.**

Сегодня у многих людей развивается телефонная зависимость, и они совершенно не представляют себе жизни без телефона.

## Видеозал

### Телефонные хулиганы

В городе появился телефонный хулиган: он совершает ложные вызовы и сообщает о несуществующем пожаре. Пожарная машина Фрэнк и скорая помощь Элис уже очень устали и хотят поскорей найти хулигана. За дело берется сыщик Роги, подключаются Руки и Пэт! Найти преступника оказывается не так-то просто!

### Телефонные мошенники

Мошенники существовали во все времена. С приходом технологий в нашу жизнь и их стремительным развитием, множились и развивались все более новые и изощренные виды.

## Мобильный этикет

**Телефонный этикет** — это правила общения по телефону, которые оставляют хорошее впечатление у других о собеседнике. Это включает в себя то, как вы приветствуете звонившего, ваш тон голоса, выбор слов, навыки слушания и умение правильно завершить звонок.

**Правила общения по телефону**

1. На телефонный звонок нужно отвечать сразу.
2. Начинать любой разговор нужно со слов приветствия: «Привет» или «Здравствуйте». Нужно представиться, назвать своё имя и уточнить, удобно ли говорить твоему собеседнику.
3. Если на том конце провода просят пригласить кого-то из близких, спрашивать: «Кто вы и зачем звоните» некультурно.
4. Если вы ошиблись номером, нужно вежливо извиниться и положить трубку. Если произошла ситуация наоборот, то не нужно смеяться и шутить над человеком, а просто сообщить, что ошиблись номером.
5. Некрасиво громко говорить по телефону в общественном месте, в котором люди соблюдают тишину (в библиотеке, в магазине, в общественном транспорте).
6. К незнакомому человеку и взрослому на том конце провода нельзя обращаться на «ты». Следует всегда говорить «Вы».
7. Ваша просьба при телефонном разговоре должна быть вежливой. Не забывайте про волшебные слова «будьте любезны» или «будьте добры», «пожалуйста», «спасибо».
8. Телефонный разговор не должен быть слишком долгим.
9. Не следует звонить по телефону утром до 8 часов или вечером (кроме случаев срочного сообщения).

**Главное: беседа по телефону должна быть вежливой и доброжелательной, понятной и краткой.**

**Мобильный этикет**

**Задание.** Телефонный разговор — это особый род общения, где есть свои правила. Попробуем разобраться в них. Найдите правильный ответ!

1. Можно ли давать номер телефона без разрешения владельца? ○ Нет ○ Только в том случае, если люди знакомы друг с другом ○ Да, конечно!

2. Кто должен перезвонить, если телефон внезапно отключился?
   ○ Неважно ○ Тот, кто звонил ○ Тот, кому звонили
3. У вас мобильный телефон. Где он будет помехой?
   - ○ В транспорте ○ На уроке ○ В театре
   - ○ В парикмахерской

4. Кто-либо по ошибке набрал ваш номер. Что вы сделаете?
   - ○ Посоветую точнее набирать номер ○ Просто положу трубку
   - ○ Отвечу: «К сожалению, вы ошиблись»

5. Какие фото нельзя выкладывать в интернет?
   - ○ Вид из окна ○ Фото паспорта ○ Фото билета в кино
   - ○ Свои рисунки

6. В какое время удобно звонить?
   - ○ После 7 утра до 11 вечера
   - ○ Если выходной, то не важно - кто-нибудь все равно есть дома ○ После 8 утра до 10 вечера

7. Вы были подписаны на какого-то блогера, но потом вы в нём разочаровались. Ваши действия: ○ Напишу в комментарии кучу советов и указаний, что ему надо делать ○ Отпишусь и просто перестану читать
   ○ Сообщу автору о том, больше в нем не заинтересован

8. По телевизору идет ваш любимый сериал, а друг позвонил, чтобы поговорить. Как вы поступите? ○ Скажу так: «Извини, сейчас не могу с тобой разговаривать. Позвоню позднее. Во сколько лучше перезвонить?»
   - ○ Поговорю немного, слушая не особенно внимательно, следя за действием на экране
   - ○ Скажу честно: «Позвони, пожалуйста, попозже, сейчас я смотрю телевизор»

9. Вы разговариваете по телефону, а в это время вам позвонили в дверь. Что делать?
   - Попрошу собеседника подождать некоторое время у телефона, пока я разберусь с посетителем
   - Открою дверь и вернусь к разговору по телефону
   - Извинюсь перед собеседником и скажу, что перезвоню попозже

**Интересные факты**

- **3 апреля** -День рождения мобильного телефона
- Люди с древности задумывались о том, как можно передавать друг другу важную информацию. В далёкие времена люди подавали сигнал, зажигая костёр на высоком холме.
- Жители Африки вместо огня барабанили в тамтамы. Звуки разносились на далёкие расстояния, причём каждый из звуков обозначал свою информацию. Древние племена галлов рассказывали новости при помощи криков, передавая информацию друг другу по цепочке. ○ В Европе церковный колокол оповещал людей о беде или радости. Самыми надёжными доставщиками информации были гонцы и почтовые птицы.
- Прежде, чем появился телефон, прошло очень много времени, была придумана масса изобретений. Создателем телефона считается американский учёный Александр Грехем Белл. У первого телефона ещё не было звонка.
- Много лет учёным предстояло совершенствовать телефонный аппарат, прежде чем появился современный сотовый (мобильный) телефон. Первый сотовый телефон появился в 1973 году в компании "Моторола", мог работать без подзарядки не более 20 минут. Он был похож на кирпич, весил почти 800 граммов.

Motorola Dynatac 8000X.

# Вредоносные программы для мобильных устройств

Давай поговорим с тобой о твоем телефоне. Точнее об опасностях для него. Существуют программы, которые могут причинить вред мобильным устройствам. С каждым годом все больше вредоносных программ появляется для мобильных устройств.

Интерес для злоумышленников представляют персональные данные пользователей, такие как номер телефона, ФИО, дата рождения. аккаунты в социальных сетях и другие личные данные.

Один из путей заражения мобильного телефона вирусом – через файл. Ты можешь получить его сам, скачав из Интернета, можешь получить по электронной почте или через мессенджер. Чтобы избежать такой ситуации, нужно проверять расширение скачанного файла. Чаще всего вирусный файл будет иметь расширение ***apk**. Еще вирус может попасть в телефон при скачивании поддельного приложения. Чтобы убедиться в подлинности приложения, зайди на официальный сайт компаниираразработчика и проверь, выпускает ли она данное приложение.

Как скачать не поддельное приложение?

1. С помощью взрослых найди официальный сайт производителя приложений.
2. Проверь, чтобы сайт работал с защищенным соединением. Для этого обрати внимание на замочек слева в адресной строке и на адрес сайта (должен начинаться с https://)
3. Вместе со взрослыми найди на странице информацию о приложении, которое тебя интересует, и ссылку на магазин приложений.
4. Обязательно изучи отзывы в магазине приложений об интересующей тебя программе.
5. При установке приложения обрати внимание на то, есть ли в нём встроенные покупки. Во многих приложениях после бесплатного пробного периода автоматически включается платная подписка. Будь внимателен при совершении покупки в приложении.

Существуют антивирусные программы для телефонов. Убедись, что на твоем компьютере, телефоне или планшете установлена антивирусная

программа, и следуй ее рекомендациям. Она защитит тебя от самых распространенных интернетатак.

# Проверь себя!

## Давайте обсудим!

**Ситуация 1.** Ты общаешься в социальной сети со своими друзьями. Неожиданно от незнакомого тебе человека приходит сообщение: «Привет, у тебя отличные фото! Только у меня все равно круче! Жми скорее сюда!». Предлагается перейти по ссылке для просмотра фотографий. Как следует поступить в данной ситуации?

**Ситуация 2.** Ты находишься в сети Интернет, изучаешь сайты с информацией о далеких планетах. Вдруг наталкиваешься на сайт, который предлагает составить твой личный гороскоп. Ты переходишь по ссылке, отвечаешь на все предложенные вопросы. В конце опроса тебе предлагается ввести номер мобильного телефона. Какими будут твои действия? Почему?

**Ситуация 3.** Тебе позвонил друг и сообщил, что увидел в интернет-сообщение о срочном сборе средств для лечения больного котёнка. Деньги предлагается перевести на счет указанного мобильного телефона или на электронный кошелек. Твой друг настаивает на помощи котёнку. Какими будут твои действия? Почему?

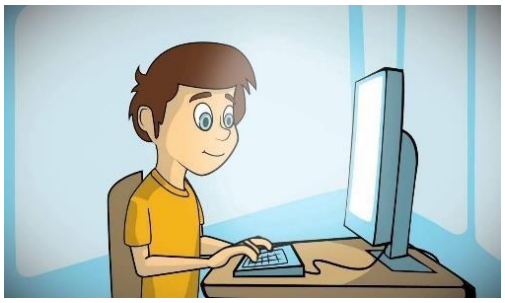
**Ситуация 4.** Во время общения в социальной сети тебе приходит сообщение: «Привет! Мы с тобой както виделись у наших общих друзей. Решил тебя найти в сетях. Классная у тебя страничка! Может пойдем вечером гулять?» Как ты поступишь в этой ситуации? Почему?

## Викторина «Что я знаю о безопасной работе Интернете»

**1.** Ученик 3-го класса Вася Паутинки зашел на незнакомый ему сайт. Вдруг на экране компьютера появились непонятные Васе сообщения. Что Васе предпринять?

a. Закрыть сайт
b. Обратиться за помощью к родителям
c. Самому устранить неисправность

**2.** Вася Паутинкин, бывая в Интернете, часто сталкивается с неприятной информацией, которая “лезет со всех сторон”, она мешает ему работать в Интернете. Как Васе избавиться от ненужной информации, чтобы пользоваться только интересными ему страничками.



a. Установить антивирусную программу
b. Установить в свой браузер фильтр
c. Установить новый браузер

**3.** Вася Паутинкин на уроке информатики создал себе электронный ящик. Теперь он может обмениваться сообщениями со своими друзьями. Сегодня на адрес его электронной почты пришло сообщение: файл с игрой от неизвестного пользователя. Как поступить Васе?

a. Не открывать файл
b. Отправить файл своим друзьям
c. Скачать файл и начать играть

**4.** Вася Паутинкин познакомился в Интернете с учеником 3 класса Иваном Неизвестным. Иван не учится с Васей в одной школе, и вообще Вася его ни разу не видел. Однажды Иван пригласил Васю, встретится с ним в парке. Что делать Васе?

a. Пойти на встречу вместе с мамой или папой
b. Не ходить на встречу
c. Пойти на встречу

**5.** Новый друг Васи Паутинкина, с которым Вася познакомился вчера в Интернете, Иван Неизвестный попросил Васю срочно сообщить ему такую информацию: номер телефона, домашний адрес, кем работают родители Васи. Вася должен:

a. Пойти на встречу вместе с мамой или папой
b. Не ходить на встречу
c. Пойти на встречу

**6.** Вася

решил опубликовать в Интернете свою фотографию и фотографии своих одноклассников. Можно ли ему это сделать?

a. Можно с согласия одноклассников
b. Можно, согласие одноклассников не обязательно

c. Нет, нельзя

**7.** Васе купили компьютер. Вася теперь целый день проводит за компьютером. Через несколько дней у него стали слезиться глаза, появились боли в руках. Что делать Васе?

a. Соблюдать правила работы на компьютере
b. Больше никогда не работать на компьютере
c. Продолжать проводить время за компьютером

**8.** У Васи Паутинкина возникли вопросы при работе в онлайн-среде. Родители Васи уехали в командировку, бабушка Васи не может ему помочь. К кому Вася может обратиться?

a. Он может спросить у одноклассников
b. Ему следует подождать приезда родителей
c. Он может обратиться на линию помощи «Дети Онлайн»

**9.** Вася Паутинкин на уроке информатики услышал новое слово “нетикет”. Что оно обозначает?

a. Правила сетевого этикета
b. Правила работы на компьютере
c. Правила этикета

**Ответы**

1. **b** - всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
2. **b** - чтобы не сталкиваться с неприятной и агрессивной информацией в Интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в Интернете.
3. **a** - Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Убедись, что на твоем

компьютере установлен брандмауэр и антивирусное программное обеспечение. Научись их правильно использовать. Помни о том, что эти программы должны своевременно обновляться.

4. **а** - Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
5. **а** - Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья! 6. **а**
7. **а** - Соблюдать правила работы на компьютере: Расстояние от глаз до экрана компьютера должно быть не менее 50 см. Одновременно за компьютером должен заниматься один ребенок. Продолжительность одного занятия – не более 60 минут. После 10–15 минут непрерывных занятий за ПК необходимо сделать перерыв для проведения физкультминутки и гимнастики для глаз. Продолжительное сидение за компьютером может привести к перенапряжению нервной системы, нарушению сна, ухудшению самочувствия, утомлению глаз. Физкультминутка для глаз
8. **с -** Если у тебя возникли вопросы или проблемы при работе в онлайнсреде, обязательно расскажи об этом кому-нибудь, кому ты доверяешь. Твои родители или другие взрослые могут помочь или дать хороший совет о том, что тебе делать. Любую проблему можно решить! Ты можешь обратиться на линию помощи “Дети онлайн” по телефону: 88002500015 (по России звонок бесплатный) или по e-mail: helpline@detionline.com. Специалисты посоветуют тебе, как поступить.
9. **а -** Нетикет (Netiquette) – (англ. Net – сеть, Etiquette – этикет)– нравственные правила поведения в компьютерных сетях. Используй при общении смайлики! :-) улыбающийся :-))) смеющийся :-D радостно смеющийся :| задумчивый, нейтральный :-( грустный :-/ недовольный или озадаченный :-O удивлённый (рот открыт).

## Игра "Безопасный Интернет"

Обезопасить себя не так уж и трудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила.

1. Сообщишь свои данные?
   a. Да
   b. Нет
2. Добавишь незнакомца в друзья?
   a. Да
   b. Нет

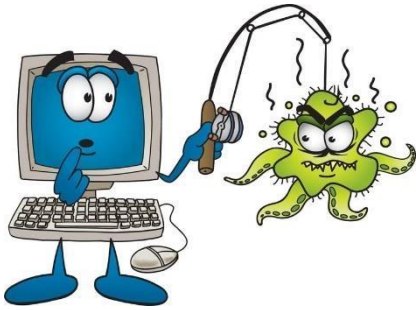
3. Посоветуешься со взрослыми, прежде чем играть?
    a. Да
    b. Нет
4. Нажмёшь без спроса неизвестные кнопки?
    a. Да
    b. Нет
5. Согласишься на личную встречу?
    a. Да
    b. Нет

**Ответы**

1. **b** - Храни в тайне свои: фамилию, номер телефона и школы, адрес, где ты живёшь, дату своего рождения, пароли и другую личную информацию.
2. **b** - Рассказывай родителям о своих друзьях в сети и советуйся, прежде чем добавить кого-то нового "в друзья" - незнакомец в Интернете также опасен, как и на улице.
3. **a** - Показывай взрослым, в какие интернет-игры ты играешь, - это поможет сберечь компьютер от вирусов, а тебя и твою семью от мошенников.
4. **b** - Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
5. **b** - Если тебя приглашают встретиться твои интернет-знакомые - соглашайся прийти только со своими родителями.

## Тест "Я и кибермошенники: кто кого?"

Пока ты читаешь этот текст, пользователи в мире скачали 47.000 приложений, ввели более 2 миллионов поисковых запросов в Google, получили 204 миллиона новых электронных писем, накупили на Amazon товаров на $83.000, опубликовали 6 новых статей в Википедии. А еще 20 пользователей во всем мире стали жертвами кражи личных данных. Проверим, насколько высоки у тебя шансы оказаться среди них в следующую минуту?



1. Каких компьютерных вирусов не бывает?
    a. Зомби
    b. Вампир
    c. Троянский конь
    d. Червь
2. Что, кроме номера карты, стремятся выведать у вас фишеры?
    a. POS-терминал
    b. DNS-сервер
    c. CVV-код
3. Вы сегодня именинник. И в лавине теплых слов от друзей в соцсети видите сообщение от незнакомого человека со словами поздравлений и ссылкой на необычную открытку – она частично отображается в сообщении, но видно плохо. Ваши действия?
    a. Пойду и посмотрю. Что плохого в открытке, пусть и не отображается
    b. Поблагодарю, но по ссылке на всякий случай кликать не буду 4. В чем разница между фишингом и кетфишингом?
    a. Это совершенно разные понятия. Фишинг – мошенничество в Сети, а кетфишинг – форма интернет-травли.
    b. Ни в чем. Кетфишинг – выдуманное слово.
5. Друг в соцсети начинает с вами банальную переписку из разряда «Привет. Как дела?», а затем присылает ссылку. Вы переходите по ней и видите ролик, как на фото, только с вашим именем и фамилией, а под ним комментарии типа «И не стыдно такое вытворять???» с аватарками ваших же друзей. Но посмотреть видео не можете – вас просят загрузить Flash Player, так как ваш устарел. Ваши действия?

a. Гляну. Я хорошо знаю этого человека, он мне точно не будет скидывать зараженное вирусами видео. Да и друзья комментировали. Грешков за мной нет, но, может, кто-то смонтировал из разной ерунды и выложил – а мне потом доказывай, что такого не было.
b. Не пойду смотреть. Лучше позвоню другу и спрошу, что за видео он мне кинул. Мало ли.

**Ответы**

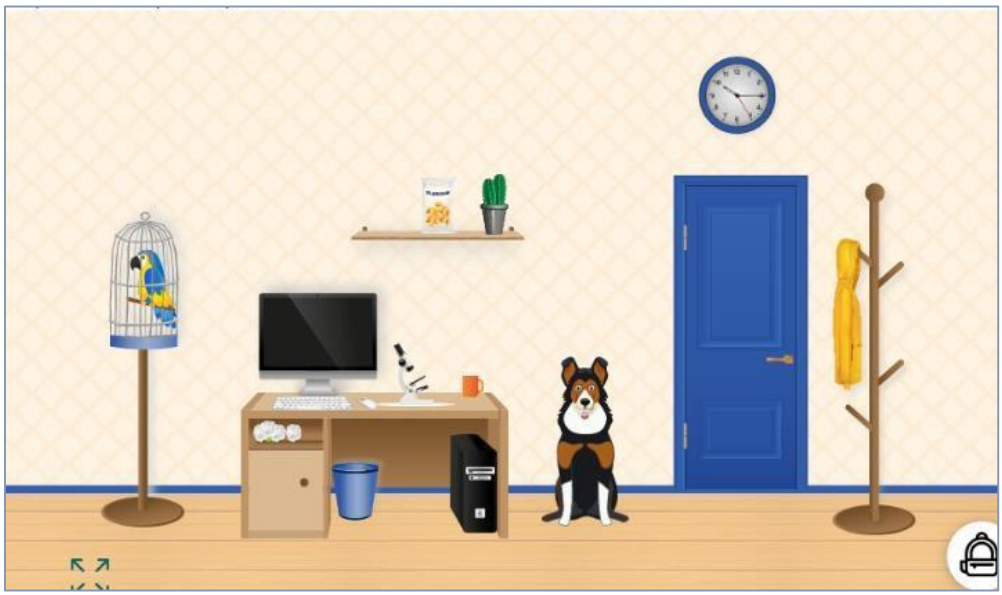
1. **b -** Пока еще не существует только вирусов-вампиров. "Черви" отличаются способностью воспроизводить себя на компьютерах через компьютерные сети, "троянские кони" прикидываются легальным ПО, а "зомби" после проникновения на компьютер управляются извне и используется злоумышленниками для организации атак на другие компьютеры.
2. **c -** CVV-код – это трехзначный код для проверки подлинности вашей карты при оплате через интернет и других видах операций, располагается он на обратной стороне карты. Именно CVV нужен злоумышленникам, чтобы потратить ваши деньги на онлайн-покупки. Никогда не называйте его никому, так же, как и ПИНкод. Ни DNS-сервер, который всего лишь выдает информацию компьютерам, как искать друг друга через интернет, ни POS-терминал, которым вы пользуетесь, расплачиваясь картой в магазине, мошенников не интересуют.
3. **b -** Не стоит переходить по ссылкам, присланным в соцсетях, тем более незнакомцами. В любой файл можно встроить вредоносный код, а ссылка на открытку вполне может перенаправить на фишинговый сайт, где у вас поросят ввести, например, пароль от вашего аккаунта в соцсети, причем для правдоподобности в качестве логина там уже может быть введен ваш e-mail или номер телефона, честно взятые с вашего аккаунта, если вы не скрыли эти данные настройками конфиденциальности.
4. **a -** Фишинг — получение мошенническим путем доступа к конфиденциальным данным пользователей, а кетфишинг — форма травли в Сети, когда киберхулиган воссоздает профиль жертвы в социальных сетях на основе украденных фотографий и других личных данных и публикует от ее имени нежелательный контент.
5. **b -** На фото реальная фишинговая страница, созданная для загрузки вредоносных программ на компьютер жертвы. Имя и фамилия, аватарки друзей и другая информация с вашего профиля вставляется сюда автоматически для правдоподобности. А переписывались вы не с другом, а с чат-ботом, работавшим со взломанной страницы вашего друга.

# WEB-Квесты по информационной безопасности

## Квест №1

Инструкция для прохождения квеста:

1. Перейдите по ссылке: https://www.learnis.ru (регистрация не требуется)
2. Войдите в созданный квест.
3. Введите номер комнаты: **742043**
4. Квест содержит 5 заданий.
5. Находите подсказки, выполняйте задания и узнавайте больше об информационной безопасности.
6. Вам необходимо открыть дверь. Кодом для открывания двери станет сумма чисел ответов на все пять заданий.



## Квест №2

Инструкция для прохождения квеста

1. Перейдите по ссылке: https://www.learnis.ru (регистрация не требуется)
2. Войдите в созданный квест.
3. Введите номер комнаты: 742172
4. Квест содержит 4 задания.
5. Находите подсказки, выполняйте задания. Ищите по комнате записки с вопросами. Их 4 ❗ Нажимайте на все, передвигайте предметы.

6. Вам необходимо открыть дверь. Кодом для открывания двери станет сумма чисел ответов на все пять заданий.
7. Записывайте номера правильных ответов по порядку вопросов (например: 4421) Это будет код от двери.
8. Подойдите к двери и набирайте код.

КВЕСТ заставит вас здорово пошевелить мозгами 🤔

Удачи всем 😜


# Полезная информация

## Толковый словарь

**Антивирусная программа (антивирус)** – любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

**Блог** (от англ. web log, «сетевой журнал или дневник событий») – сайт, онлайндневник, содержащий регулярно добавляемые записи, ссылки, изображения или мультимедиа в обратном хронологическом порядке.

**Блокировка, занесение в «черный список»** – функция многих интернет-сервисов, например социальных сетей, форумов. Пользователь, которому присвоен такой статус, теряет право посылать Вам сообщения, смотреть Вашу страницу.

**Браузер** (от англ. web browser) – программное обеспечение для просмотра вебсайтов, т. е. для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой.

**Веб-сайт, сайт** (от англ. website: web – паутина, сеть; site –место, букв.: «место, сегмент, часть в сети») –совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединенных под одним адресом.

**Вредоносная программа** – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам компьютера или к информации, хранимой на компьютере, с целью использования ресурсов компьютера или причинения вреда (нанесения ущерба) владельцу информации.

**Кибербуллинг (кибертравля)** – агрессивное, умышленное действие, совершаемое группой лиц или одним лицом с использованием электронных форм контакта, повторяющееся неоднократно и продолжительное во времени в отношении жертвы, которой трудно защитить себя.

**Кибермошенничество** – один из видов киберпреступления, целью которого является умышленный обман или злоупотребление доверием пользователей с целью получения какой-либо выгоды.

**Компьютерный вирус** – разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликации). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные пользователя, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

**Контент** (от англ. content – содержание, содержимое) – любое информационно значимое наполнение или содержание какого-либо информационного ресурса: текст, графика, музыка, видео, звуки и т. д.;

**Мобильный контент** – мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефонах, смартфонах, коммуникаторах и т. д.), – текст, графика, музыка, рингтоны, видео,

игры, дополнительное программное обеспечение. Для контента важными параметрами являются объем, актуальность, доступность, дизайн, привлекательность.

**Мессенджер** (от англ. messenger – связной, курьер) – система мгновенного обмена сообщениями – группа программ для обмена сообщениями в реальном времени через интернет.

**Онлайн** (англ. online, от англ. on line – на линии, на связи, в Сети, в эфире) – находящийся в состоянии подключения. В отношении программного обеспечения почти всегда означает «подключенный к интернету» или «функционирующий только при подключении к интернету». Также – происходящее в интернете, существующее в интернете. Является антонимом термину офлайн.

**Социальная сеть** – программный сервис, площадка для взаимодействия людей в группе или в группах; сайт, объединяющий отдельных людей или организации. Ее участники реальны и связаны друг с другом теми или иными отношениями: от случайных знакомств до тесных семейных и дружеских связей. В качестве подобия социальной сети можно рассматривать любое онлайн-сообщество, члены которого участвуют, например, в обсуждениях на форуме. Социальная сеть также образуется читателями тематического сообщества, созданного на любом сервисе блогов. Многие профессиональные сообщества превратились в инструмент поиска людей, рекомендации сотрудников и поиска работы.

**Спам** (от англ. spam) – анонимная массовая не запрошенная рассылка коммерческой, политической и другой рекламы или иного вида сообщений от неизвестных людей или организаций без согласия получателя.

**Троллинг** (от англ. trolling – блеснение, ловля рыбы на блесну) – размещение в интернете (на форумах, в дискуссионных группах, социальных сетях и др.) провокационных сообщений с целью вызвать конфликты между участниками, оскорбления. Лицо, занимающееся троллингом, называют троллем, что совпадает с названием мифологического существа.

**Файл** – основной элемент хранения данных в компьютере, позволяющий находить, изменять, удалять или выполнять с ним другие операции. В файлах могут храниться тексты, документы, программы и любые другие данные.

**Форум** – интернет-сервис для общения (обычно на определенную тему), где каждый пользователь может оставлять свои текстовые сообщения,

доступные для прочтения другим. Форум отличается от чата разделением обсуждаемых тем и возможностью общения не в реальном времени. Форумы часто используются
для разного рода консультаций, в работе служб технической поддержки. В настоящее время форумы являются одним из наиболее популярных способов обсуждения вопросов в интернете.

**Чат** (от англ. to chat – болтать, болтовня, разговор) – средство обмена сообщениями между двумя или более участниками по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.

**Шпионские программы** – программное обеспечение, при помощи которого осуществляется сбор информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

## Памятки

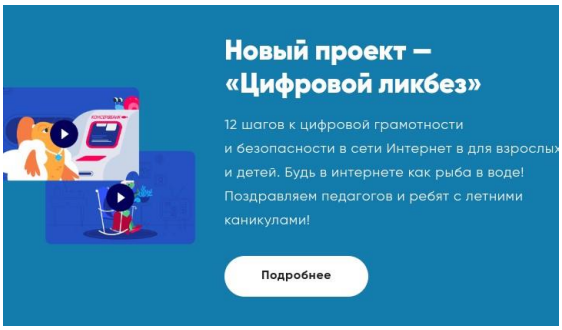
- Как безопасно играть online **(скачать) (посмотреть)**
- Как безопасно общаться в социальных сетях **(скачать) (посмотреть)**
- Как безопасно пользоваться сетью Wi-Fi **(скачать) (посмотреть)**
- Как безопасно пользоваться смартфоном, планшетом **(скачать) (посмотреть)**
- Как безопасно пользоваться электронной почтой **(скачать) (посмотреть)**
- Как безопасно расплачиваться электронными деньгами **(скачать) (посмотреть)**
- Как защитить свою цифровую репутацию **(скачать) (посмотреть)**
- Как защититься от кибербуллинга **(скачать) (посмотреть)**
- Как защититься от компьютерных вирусов **(скачать) (посмотреть)**
- Как защититься от фишинга **(скачать) (посмотреть)**
- Что такое авторское право **(скачать) (посмотреть)**

## Чат-бот по кибербезопасности


МТС в рамках проекта «Дети в Интернете» запустил голосовой чат-бот по кибербезопасности. В Telegram популярные блогеры рассказывают о возможных онлайн-опасностях и о том, как их можно избежать. Главная задача сервиса — научить детей основам правильного и безопасного поведения в Сети. Обучающий чат-бот находится в мессенджере Telegram — @cybersafety_bot. На онлайн-платформе шесть популярных блогеров через голосовые сообщения говорят о разных аспектах безопасности в интернете. Пользователь может выбрать одного из «наставников», тему для изучения и начать «беседу».

Как правильно общаться с незнакомцами в интернете и не стать участником опасного челленджа? Почему так важно следовать онлайн-этикету? Как защитить свой аккаунт от злоумышленников? Что делать, если столкнулся с травлей в интернете? На эти и другие вопросы блогеры дадут простые и понятные ответы. После завершения общения по каждой теме пользователи чат-бота получат ссылку на серию видеороликов проекта «Дети в интернете», которые позволяют получить ещё больше полезной информации о кибербезопасности.

## 12 шагов к цифровой грамотности для взрослых и детей от Урока Цифры




Телефонное мошенничество

Интернет-мошенничество

Интернет-травля

Кража денежных средств

Компьютерные и телефонные вирусы

Работай с информацией эффективно

Используй достоверные источники информации

Общайся в соцсетях и мессенджерах безопасно

Покупай в интернете легко и безопасно

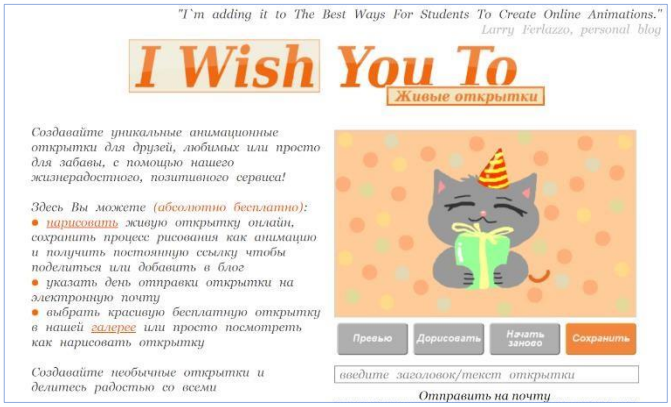
Повысь свою финансовую грамотность

**Расскажи детям о цифровых навыках**

**Учи детей учиться**

# Компьютер мой друг и помощник

## Рисуем живую открытку




Сервис на русском языке **Iwishyouto** позволяет создавать оригинальные анимационные открытки. Возможности сервиса для создания «живых» открыток: нарисовать свою живую открытку, сохранить процесс рисования как анимацию и получить постоянную ссылку на нее и код для встраивания открытки на странички сайтов или блогов.

## Рисуем на компьютере

**Поэтапное рисование щенка**

**Поэтапное рисование птички**

## Раскраски

Смайлики – это весёлые и забавные рожицы, которые выражают самые разные эмоции. Смайл может не только улыбаться и грустить, но и смеяться до упаду, лить слёзы, стесняться и злиться.


Обычно изображение смайлика – это жёлтый круг с черными глазами. Но маленькие художники могут выбрать для раскрашивания любой другой понравившийся цвет.

Скачать и распечатать можно абсолютно бесплатно на этом **сайте**.

А это **раскраска** с простыми советами по безопасному использованию Интернета.

## Как превратить текст в эмодзи

Сегодня мы рассмотрим онлайн сервис, при помощи которого можно превратить любой текст в симпатичный рисунок в стиле эмодзи. Итак, заходим на **страницу сервиса** и сразу же попадаем в редактор.


В верхнем окошке надо написать текст при помощи клавиатуры. В правой части можно выбрать символы, при помощи которых вы хотите сделать отображение надписи. В нижней части редактора – опции для настройки шрифта и скачивания готового рисунка.

Как же выглядит текст в стиле эмоджи? Вот несколько примеров.


Таким образом можно написать свое имя, составить поздравление, небольшое послание и пр. В любом случае это будет выглядеть необычно и привлекательно).

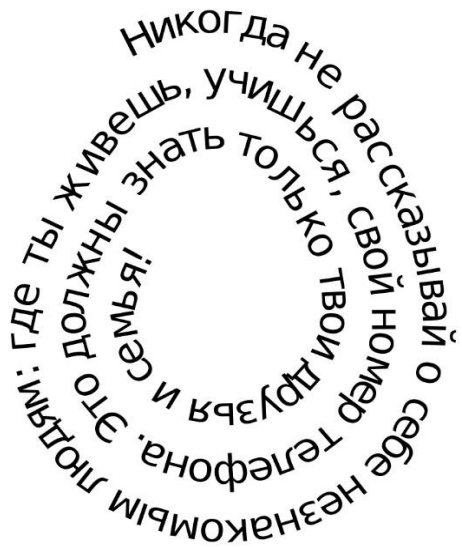

Сразу хочу обратить Ваше внимание на такую особенность: по умолчанию редактор не отображает текст, набранный на кириллице. Для исправления этого щелкаем по кнопке «Font» и в выпадающем списке выбираем «Unicode».

При помощи остальных кнопок Вы можете задать размер шрифта (Size), размер и плотность отображения картинок (Pattern и Density), фон (Background), заданный стиль (Styles).

Скачать готовую картинку с текстом в стиле эмоджи можно при помощи кнопки «Download».

## Урок скорочтения от смайлика

Чтение по спирали? Не так-то это и легко! Надо сконцентрировать свое внимание и удерживать его до конца чтения! Надо читать осознанно, по крупицам собирая буквы в слова и запоминая их общий смысл! В этих текстах зашифрованы правила безопасности в Интернете! А еще это отличная разминка для шейного отдела позвоночника! И, наконец, это просто весело и занимательно!







## Игры с искусственным интеллектом

Google Ai Draw создал программное обеспечение, которое превратит ваши каракули в удивительные рисунки.

Программное обеспечение мгновенно распознает ваши каракули и предлагает более четкую версию вашего рисунка с помощью алгоритма искусственного интеллекта, который можно увидеть в Quick Draw. Посетите веб-сайт **AutoDraw** и ознакомьтесь с тем, как работает программное обеспечение.

Не забудьте поделиться с друзьями! 😉

Приложение абсолютно бесплатное и работает на всех устройствах.

Благодаря **И**скусственному **И**нтеллекту (ИИ) AutoDraw может распознавать изображения и находить им пару среди готовых картинок, подготовленных дизайнерами. Безусловно, искусственный интеллект далек от совершенства и также может ошибаться. Тем не менее, несмотря на редкие ошибки, AutoDraw отлично справляется с задачей и распознает даже очень плохо нарисованные объекты.

**Рисовать в AutoDraw**

Такая же технология использовалась в проекте Quick, Draw, где ИИ за 20 секунд должен был угадать, что рисует пользователь.

Что это за игра?

Игра Quick, Draw! использует технологии машинного обучения. Вы рисуете предмет, а нейронная сеть пытается угадать, что это такое. Не все ее попытки удачны. Чем чаще вы играете, тем больше знает сеть. Пока она умеет распознавать всего несколько сотен предметов, но со временем их список расширится. Эта игра – пример того, что машинное обучение может быть занимательным.

**Рисовать в QuickDraw**

## Делу время - потехе час

## Игротека

Анаграммы

Рисуем смайлами

Раскраски онлайн

Планета ребусов

Смайлобой

Угадай мультфильм

Шифровальщик

Шифровальщик 2

Шифровальщик 3

## СмайликТВ

Телеканал «Смайлик» — самый добрый и улыбчивый друг всех мальчишек и девчонок.

Детский телеканал «Смайлик» — это уникальный канал для детей в возрасте от 3 до 12 лет, наполненный исключительно полезным, познавательным, развивающим и развлекающим контентом.

Создатели и постоянная редакция телеканала «Смайлик» — это настоящие профессионалы своего дела. В команде собрались одни из самых опытных авторов, режиссёров, операторов и продюсеров в сфере детского телевидения.

Основная задача телеканала «Смайлик» — принести в каждый дом вечные ценности и традиционные основы воспитания детей. Воспитать в них доброту, чистоту и любовь к своей семье, стране и ко всему миру. Наш поистине безопасный контент наполнен позитивом и призван взращивать самые светлые чувства у чуткой и требовательной детской аудитории.

Телеканал «Смайлик» приглашает всех мальчишек и девчонок отправиться в путешествие по миру анимационных и художественных фильмов, сказок и уникальных программ собственного производства, которые не найти ни на одном другом телеканале.

**Безопасное телевидение для детей — в каждом доме!**

## Для любителей комиксов

**Комиксы «Приключение Стёпы в Интернете»**

**Супер Юни и его друзья в Интернете**

## Кинотеатр Эмодзи

**«Красавица и Чудовище» в пересказе Emoji**

Встречайте emoji-версии Белль, Чудовища, Люмьера, Когсворта и других полюбившихся персонажей, которые перескажут сюжет анимационного фильма Disney «Красавица и Чудовище».

**«Рапунцель» в пересказе Emoji**

Встречайте emoji-версии Рапунцель, Флина Райдер, Максимуса, Паскаля и других полюбившихся персонажей, которые перескажут сюжет анимационного фильма Disney «Рапунцель».

**«Холодное сердце» в пересказе Emoji**

Встречайте emoji-версии Анны, Эльзы, Олафа и других полюбившихся персонажей, которые перескажут сюжет фильма Disney «Холодное сердце».

**«Золушка» в пересказе Emoji**

Встречайте emoji-версии героев классического анимационного фильма Disney «Золушка»!

**«Аладдин» в пересказе Emoji**

Встречайте emoji-версии Аладдина, Жасмин, Джинни, Абу и других полюбившихся персонажей, которые перескажут сюжет классического анимационного фильма Disney «Аладдин».

**«Моана» в пересказе Emoji**

Встречайте emoji-версии Моаны, Мауи и других полюбившихся персонажей, которые перескажут сюжет фильма Disney «Моана».

## Азбука цифровой грамотности от Смешариков

**Азбука**

# Игры на перемене и не только...

## Игра "Испорченный телефон"

Известная игра подходит для изучения слов, связанных с темами цифровой безопасности.

Ведущий игры называет слово следующему игроку. Тот должен передать услышанное слово следующему. И так до последнего игрока, который всем громко говорит слово. Если это слово оказалось неверным, то ищут того, кто слово «сломал».

Затем обсуждается значение этого слова и его связь с цифровой безопасностью.

## Игра "Съедобное /несъедобное" (в новой версии)

Игра очень похожа на старую известную игру "Съедобное/несъедобное". Игроки образуют круг. У ведущего есть мяч. Идея игры заключается в том, чтобы правильно определить, что можно/нельзя делать в интернете/умном устройстве. Ведущий сначала произносит утверждение и делает небольшую паузу, прежде чем бросить мяч игроку. Если это действие, которое можно выполнить в Интернете, мяч принимается от ведущего. Если нет, мяч не принимается. Можно и наоборот :)

**Утверждения для использования в игре:**

- Я всегда отключаю зарядное устройство для смартфона, когда заканчиваю зарядку устройства.
- Я не использую смартфон во время еды.
- Если я получаю сообщение на смартфон, которое я не понимаю, я прошу помощи (например, мама, папа)
- Сломанный телефон можно выбросить в обычный мусор, ведь это такой же мусор, как обертки от мороженого
- Время использования компьютера должно быть ограничено, иначе глаза будут болеть, и спина вырастет горбом.
- Предметы домашнего обихода не публикуются в Интернете ни в виде изображений, ни в виде видео.
- Я загружаю случайные приложения, потому что они такие классные.
- Я делюсь паролем или шаблоном безопасности моего смартфона или смартфона моих родителей с другом, потому что все доступно для друзей.
- Ночью кладу телефон под подушку, на сон это не влияет.
- Я принимаю всех, кто хочет быть моим другом, в друзья онлайн.
- Я использую телефон друга или родителя, чтобы изменить его обои.  Играю на телефоне, пока голова не болит.

**След**

Каждый игрок обводит контур своей стопы на листке бумаги. Потом вырезает собственный след. В нём нужно нарисовать действия, которые он выполняет онлайн (персонажи, игры или устройства, которые они используют). После этого можно устроить выставку следов.

**ИДЕИ для обсуждения:**

- У всех ли нас одинаковые следы? (Некоторые больше, некоторые меньше и т. д.)
- Из чего состоит чей-то цифровой след? (Что нарисовано и изображено? Устройства, игры, персонажи и т. д.)
- Чем мой цифровой след отличается или похож на след моего друга?
- Каких следов должно быть больше? Цифровые или реальные следы?
- Как мы можем сделать больше таких реальных следов? (Меньше находиться за экранами.
- Какие могут быть приятные занятия, которые отвлекут нас от экранов :))

## Игра "Объяснялки"

"Правила сетевого этикета или КАК ОБЩАТЬСЯ В СЕТИ"

**Описание игры:**

- Игроки садятся в круг, а ведущий бросает кубик. Изображение/текст, оставшиеся на костях, обсуждаются вместе.
- Следующий бросок производит следующий игрок.
- Кубиков может быть больше и с разными темами.

- Вы можете придумывать вопросы и картинки для этой игры по своему желанию.  Дети могут вырезать кубик и склеить его.

**Кубик можно скачать здесь Можешь сделать свой кубик**

## Подведем итоги

**ПОДУМАЙ, ПРЕЖДЕ ЧЕМ ПУБЛИКОВАТЬ!**

Публикуй в интернете как можно меньше информации о себе. Будь особенно осторожен со своими паролями. Держи их при себе.

**БУДЬ МУДРЫМ!**

Помни, что информация в интернете не всегда достоверна. Сравни найденную информацию с другими источниками или обратись за советом к родителям или учителям.

**БУДЬ НАЧЕКУ!**

Открытие писем, сообщений, документов, фотографий или видео, отправленных незнакомцами, может быть опасным — они могут содержать вирусы, быть незаконными или не соответствовать вашему возрасту.

**ПОДУМАЙ ОБ ЭТОМ!**

Люди в интернете иногда выдают себя за других. Тщательно продумай первую встречу в реальной жизни с новым другом из интернета – заручись согласием родителей и возьми с собой хорошего друга. Для встречи нужно выбрать общественное место.

**ЗАЩИЩАЙ СЕБЯ!**

Если ты увидишь или услышишь в интернете что-то тревожащее тебя, то не замалчивай это, а обсуди с человеком, которому ты доверяешь. **ТЕБЕ ПОМОГУТ:**

1. Линия помощи «Дети онлайн» по телефону 8-800-250-00-15 (с 9 до 18 по рабочим дням, время московское) (звонки по России бесплатные). По электронной почте helpline@ detionline.com. На сайте **www. detionline.com.**

2. Горячая линия Центра безопасного Интернета в России (по приёму анонимных сообщений о противоправном контенте доступа). По адресам: **www.saferunet.ru**, **www.rushotiine.ru**

**Молодец! Теперь ты прошёл курс и к Интернету готов! И не забывай: будь осторожен в сети, точно так же, как и в реальной жизни!**