



«Безопасный интернет»

ПОДГОТОВИЛА: ВОЛКОВА КРИСТИНА
СЕРГЕЕВНА

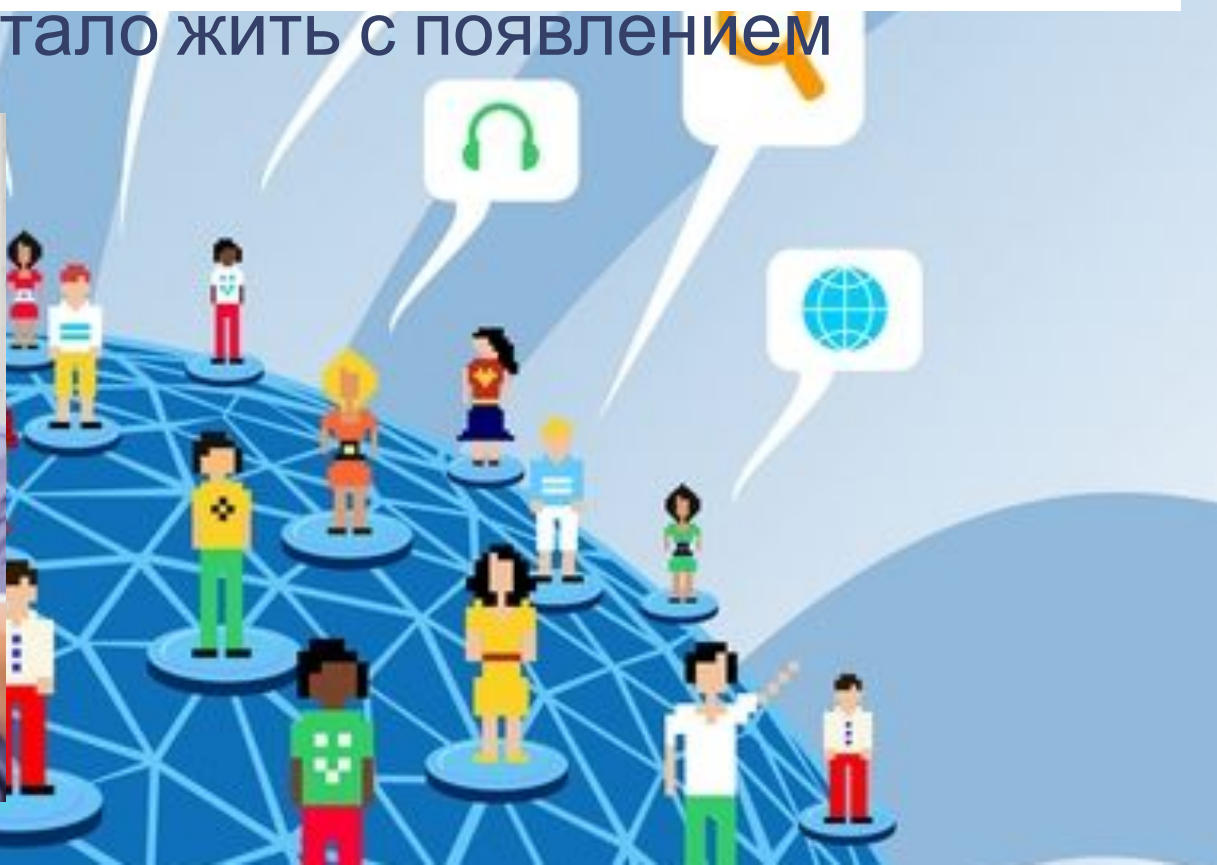
УЧЕНИЦА 9 «А» КЛАССА
МБОУ «ШКОЛЫ №6»

Богородский район, г. Богородск



В настоящее время люди с трудом представляют свою жизнь без современных гаджетов. Почти невозможно выйти из дома, например, без смартфона или ноутбука. Эти устройства стали важной частью нашей жизни.

А как легко стало жить с появлением Интернета





Что же такое интернет?



Интернёт (англ. Internet)— всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть.

Сайт ru.wikipedia.org

Интернет - Всемирная компьютерная сеть электронной связи, позволяющая пользователям персональных компьютеров, находясь на любом расстоянии, в любой точке земного шара, иметь связь друг с другом, принимать и передавать текстовую и изобразительную информации.

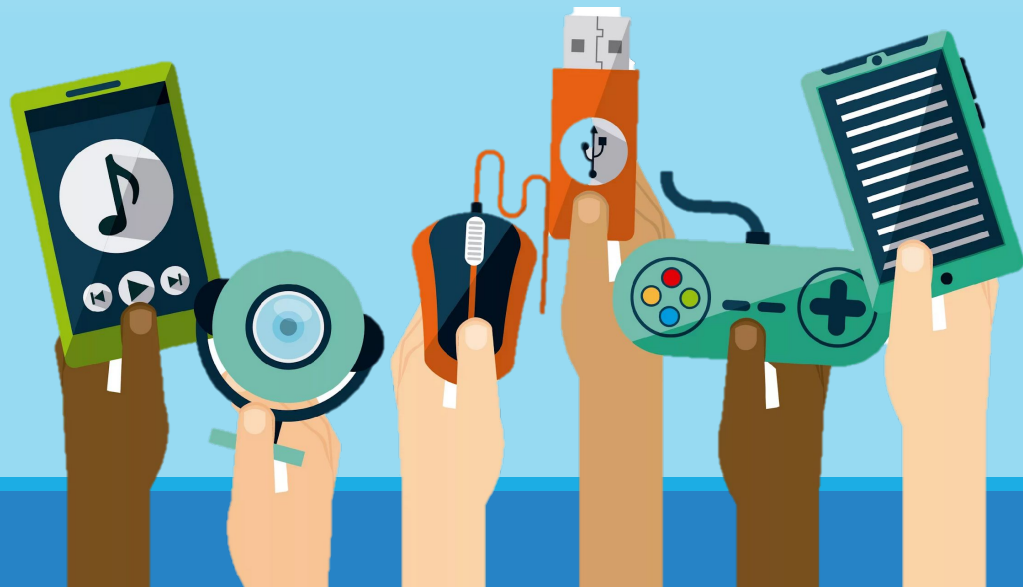
Большой современный толковый словарь русского языка.

2012



Но часто ли вы задумываетесь о том, что Интернет — это не только источник информации и возможность общаться на расстояние, но и угроза компьютерной безопасности?

Предлагаю вам поподробнее разобраться с некоторыми угрозами, подстерегающими нас во Всемирной паутине и в том, как их избежать!



Основные угрозы безопасности детей в сети Интернет.

**Кибербуллинг
(интернет-травля)**



**Вредоносные программы
(Вирусы)**



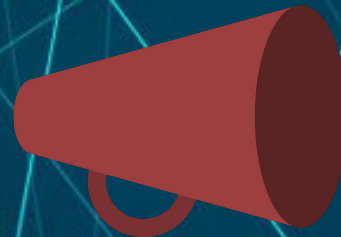
**НЕБЕЗОПАСНЫЕ
СДЕЛКИ**



Интернет-мошенники



**Опасная
реклама**



**КИБЕРШПИОН
АЖ**



Рассмотрим угрозу

- **Вредоносные программы**

Вирусы (Вирусы) – распространенное на сегодня явление. Они могут попадать на ПК с письмами по электронной почте или внутри скачанных файлов с Интернет ресурсов. Если пользователь получил письмо от неизвестного адресата с каким-то вложением, довольно велика вероятность того, что оно содержит вирус. Делается подобное для того, чтобы выкрасть какую-либо важную информацию у пользователя. Особенно опасны троянские вирусы (или «трояны»).

Их **основная задача** кража информации, а также уничтожение файлов и папок на зараженном компьютере.

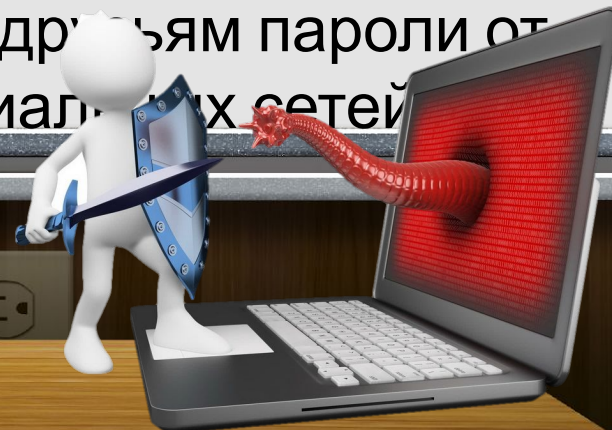




Чтобы избежать проникновения вирусов на устройство:



- Следите за регулярным обновлением операционной системы. Если этого не происходит, вирусам легче найти уязвимые места и проникнуть в компьютер.
- Пользуйтесь антивирусными программами. Они устранят многие угрозы, подскажут, можно ли посещать неизвестный вам сайт, проверят файлы, скачиваемые из интернета. Старайтесь не сообщать даже близким друзьям пароли от личного кабинета, банковских карт, социальных сетей, рабочей и личной почты.



• Продажи и покупки в интернете

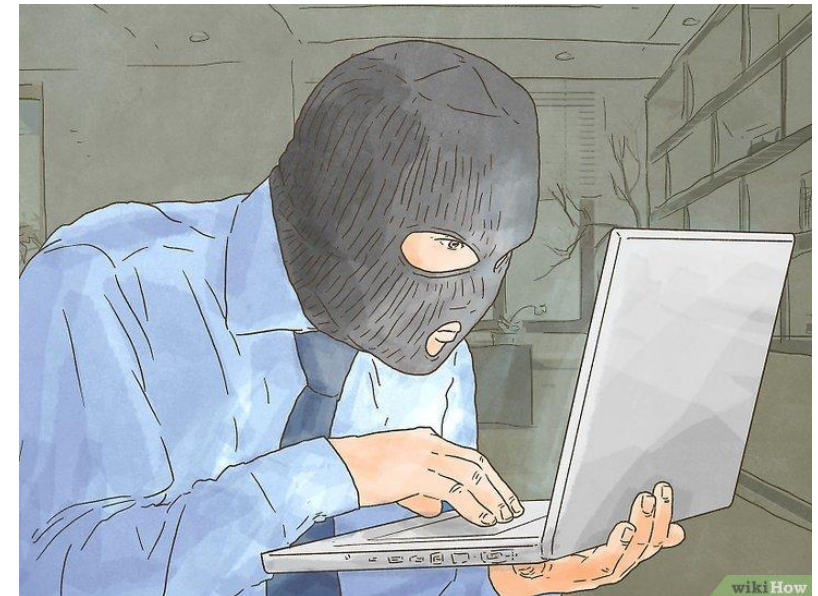
Покупать и продавать через интернет **удобно**.

Но при этом — опасно.

Вы разместили объявление на популярном сайте?

Не спешите радоваться, если вам позвонит покупатель, готовый немедленно приобрести ваш товар. Он сообщит, что хочет прямо сейчас перевести на вашу карту необходимую сумму. Всё, что от вас требуется — это реквизиты и несколько кодов, которые придут на ваш телефон.

Псевдопокупатель исчезнет сразу же, как вы отправите ему кодовое слово или пароль, пришедшие по смс. Такая **история закончится обнулением счёта вашей карточки.**

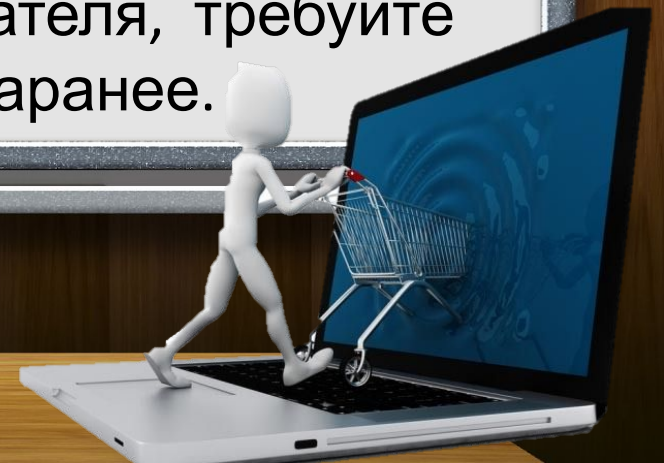




Чтобы обезопасить себя от мошенничества с банковскими картами, помните:



- Нельзя сообщать посторонним людям секретную информацию, размещённую на обороте вашей дебетовой или кредитной карты.
- Для совершения операции по оплате достаточно фамилии, имени и отчества держателя карты, а также номера карты.
- Если у вас возникает хотя бы малейшее сомнение в добросовестности продавца или покупателя, требуйте личной встречи и не передавайте деньги заранее.



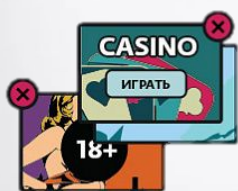
- **Раздражающая и опасная реклама**

Назойливая реклама преследует нас повсюду. Каждый сталкивался с ситуацией, когда перед видео на YouTube необходимо просматривать 30-секундный рекламный ролик. Это не только отвлекает от работы, мешает просматривать сайты, вести переписку: загрузка рекламного сообщения на вашем экране (будь то преролл или баннер) съедает часть вашего интернет-трафика. Получается, что за эту рекламу вы еще и платите. Часто из-за большого веса рекламных сообщений, сайты грузятся дольше. От этого у смартфонов значительно сокращается заряд батареи. Кроме того, реклама может содержать вредоносный код или вести на сайты с таким кодом.

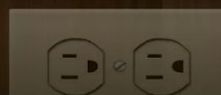




Для того, чтобы убрать рекламу при использовании Интернета уже существует множество программ и дополнений к браузерам!



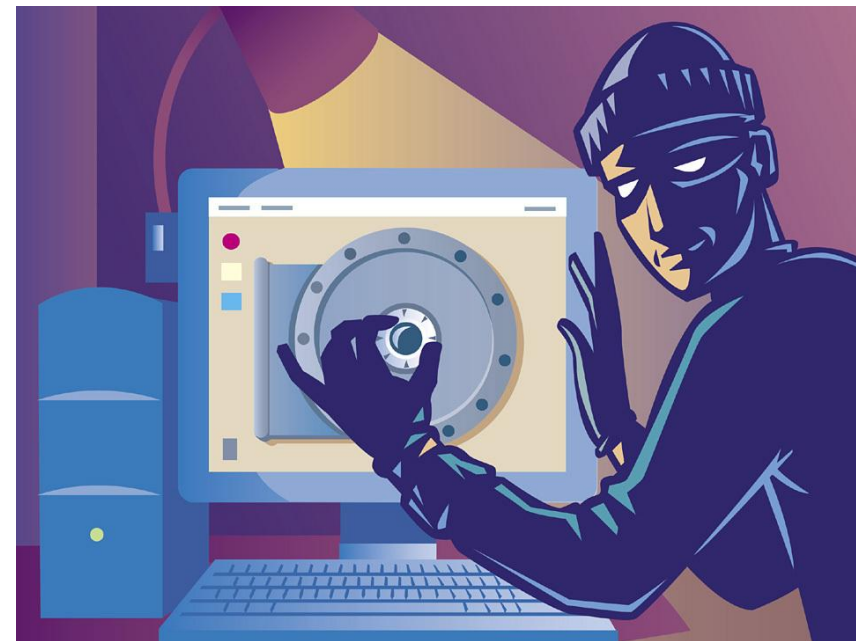
**Но будьте осторожны,
скачивая их, тщательно
проверьте отзывы и работу
выбранного сайта.**



• Кибершпионаж

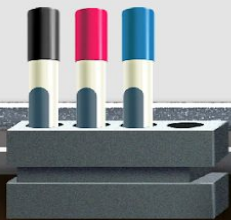
Программы-шпионы проникают в компьютер вместе с подозрительным контентом, который вы скачиваете из сети. Шпионы собирают личные данные, анализируют ваши действия, составляют список часто посещаемых сайтов, просматривают поисковые запросы, а затем отправляют эту информацию поставщикам интернет-услуг. Такие программы работают в фоновом режиме и, как правило, не заметны для обычных пользователей.

Вам может показаться, что шпионы безвредны, но это не так. Они способны **отключить антивирус**, а также **передать ваши данные злоумышленникам**.





Чтобы избежать знакомства с программами-шпионами, старайтесь не устанавливать на компьютер условно-бесплатные программы и не нажимайте на рекламные ссылки, которые открываются во всплывающих окнах.

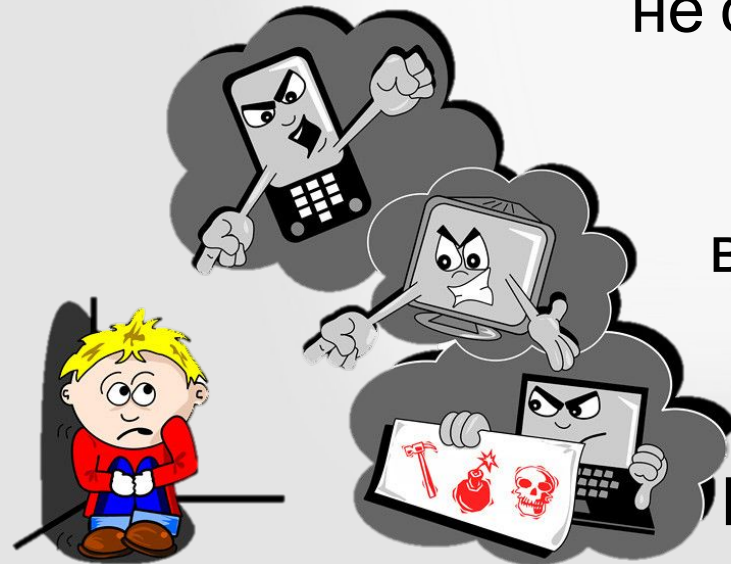


• Кибербуллинг (интернет-травля)

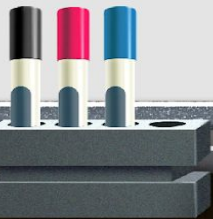
Это травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить кибербуллинг (другое название - **троллинг**) могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

«**Троллинг**» может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. В интернете, как правило, ребенок находится один на один с потенциальным обидчиком, который к тому же уверен в своей анонимности и может действовать более нагло.





По мнению эксперта «Лаборатории Касперского», борьба с кибертравлей технически не так проста, поэтому и программный родительский контроль не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются за помощью к взрослым, будучи запуганными угрозами, либо просто из-за отсутствия доверия к близким людям. Поэтому самую важную роль в защите ребенка от кибер-террора играют отношения с родителями.



• Интернет-

мошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).



В интернете мошенничество происходит чаще всего под такими предложениями:

1. Заработок.
2. Помощь нуждающимся.
3. Разблокировки опций программ, приложений.
4. Выгодное приобретение товаров.
5. Розыгрыш ценных призов.





Как не попасться на удочку к непорядочным людям и избежать мошенничества?

□ Не верьте обещаниям огромной выгоды!

Это касается предложений заработать миллионы, отдав пару тысяч рублей и сенсационных скидок! Если кто-то придумал работающую схему большого заработка при минимальных вложениях, зачем ему делиться ею с вами? Все скидки – это хорошо продуманный маркетинговый ход. Ни один продавец не станет отдавать товар ниже себестоимости!

□ Берегите личные данные!

Не стоит без реальной нужды разглашать личные данные. Если на сомнительных ресурсах вас просят ввести данные, не соглашайтесь! Опытные мошенники даже минимум информации могут превратить в собственную выгоду.

□ Не реагируйте на сообщения и звонки с незнакомых номеров!

Если вы получили сообщение с просьбой отправить деньги, перейти по ссылке, перезвонить. Не реагируйте! Даже если сообщение интригует, пугает или веселит! Это обман! Мошенники вызывают у вас сильные эмоции для того, чтобы было легче выманить вожаделенные деньги.

Подведем итоги

✓ Вряд ли кто-нибудь сможет перечислить все способы, как обманывают в интернете! Только внимательность и недоверие к тем, кто просит, убеждает и предлагает, сможет по-настоящему уберечь от мошенников!

✓ В общем, угроз и опасностей в сети хватает. Но даже учитывая все недостатки Всемирной сети, невозможно отрицать всю пользу, которую она приносит. Ей можно пользоваться, а можно и нет, но не признавать повсеместную интеграцию ее в жизнь современного общества уже невозможно.



**СПАСИБО ЗА
ВНИМАНИЕ!!!**