
интернет - может быть опасным
Интернет -угрозы
Кибер-безопасность

В России насчитывается около 8-10 млн. пользователей Интернета в возрасте до 14 лет, (среди школьников интернетом пользуются 90% учащихся);

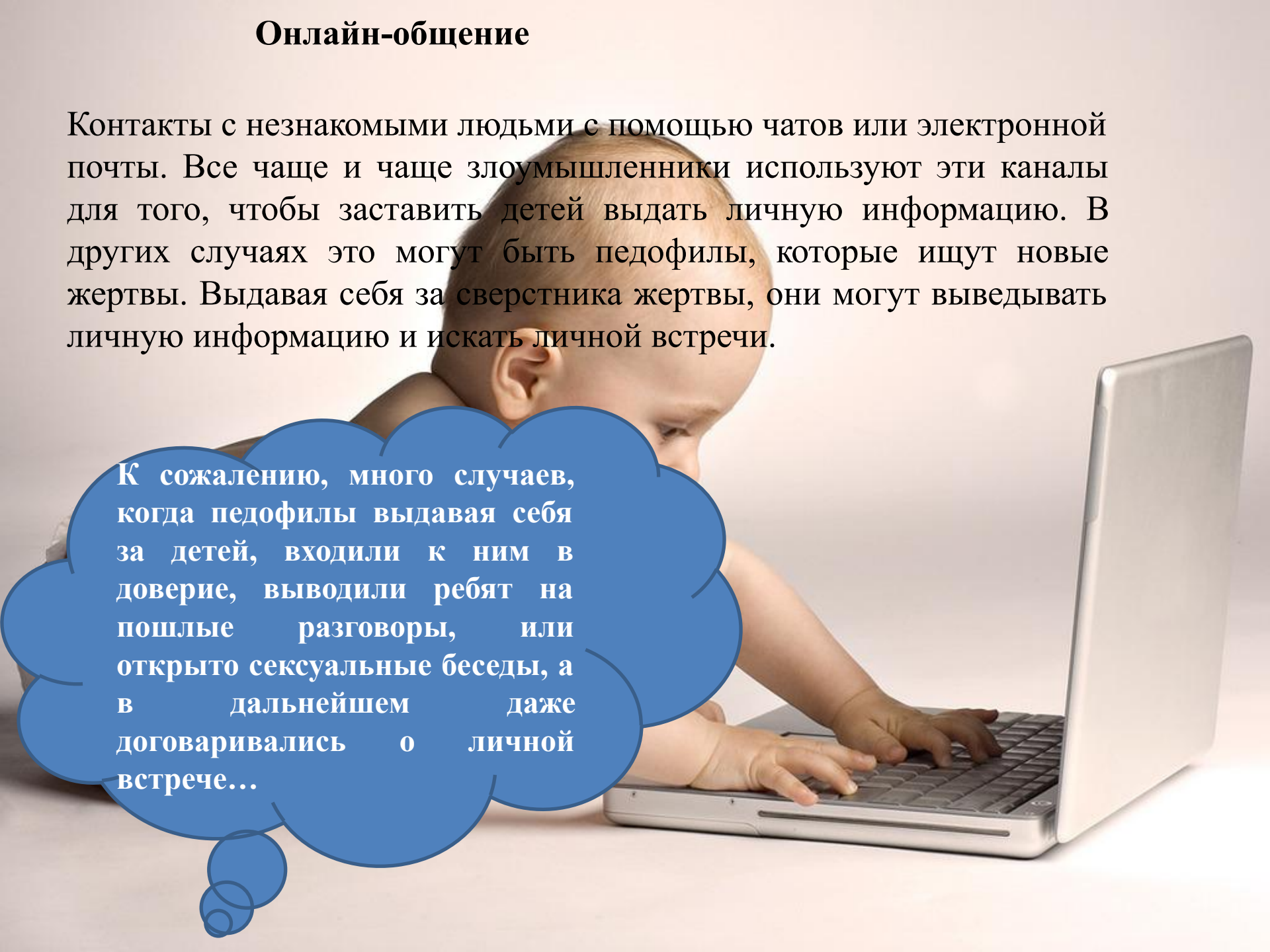
- в среднем по России дети начинают выходить в сеть в 10 лет;
- 25% пятилетних детей используют Интернет;
- порядка 6,3 млн. детей выходят в Интернет из школы;
- две трети детей, выходящих в сеть из дома, делают это самостоятельно;
- родительский контроль над пользованием ребёнком Интернетом сохраняется до 11 лет.

КИБЕРБУЛЛИНГ

В сети Интернет, как и в обычной жизни, встречаются злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, устроить травлю. Такие люди могут встретиться на форумах и чатах. Сложное слово кибербуллинг в современном мире как раз и означает преследование человека сообщениями, содержащими оскорбления, агрессию, запугивание. Лучшая защита – предупреждение!

Онлайн-общение

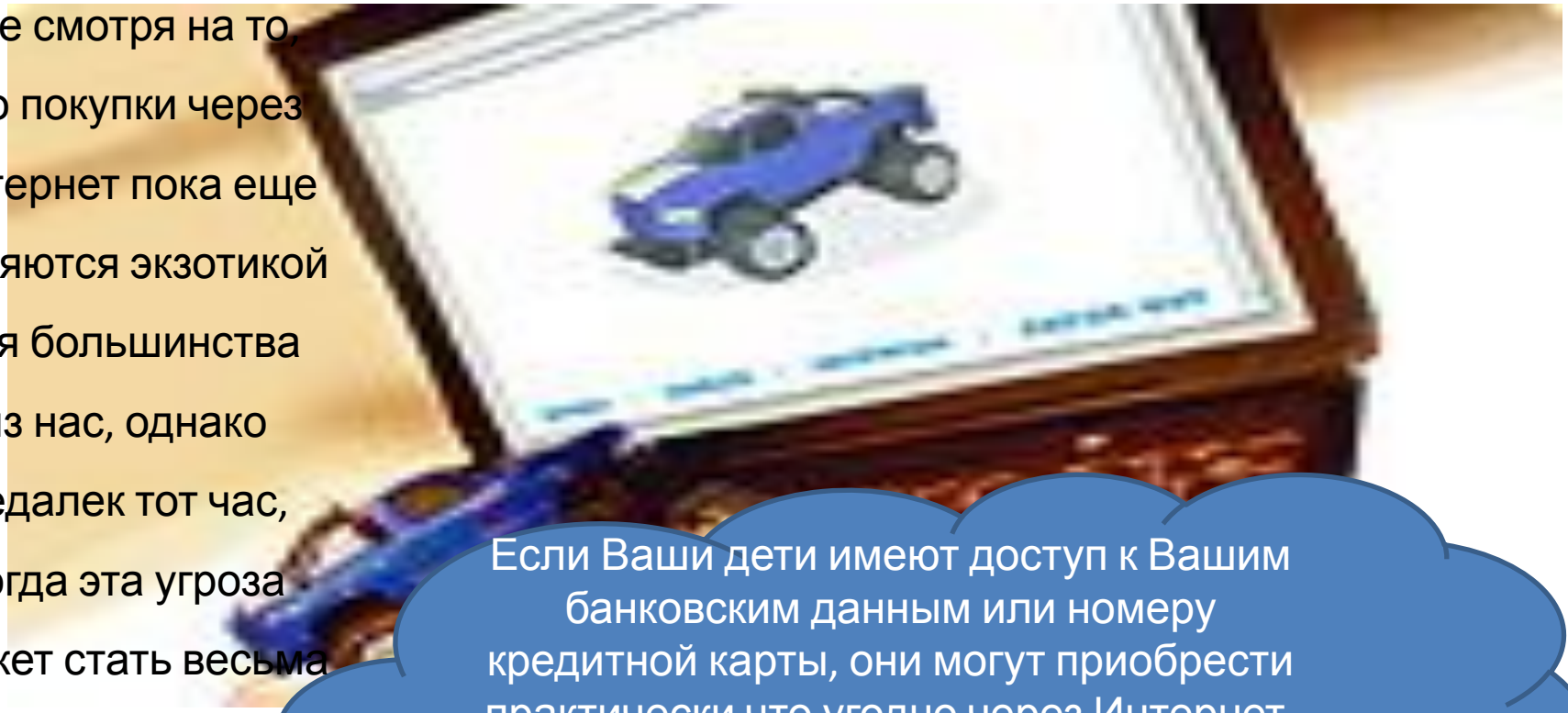
Контакты с незнакомыми людьми с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.



К сожалению, много случаев, когда педофилы выдавая себя за детей, входили к ним в доверие, выводили ребят на пошлые разговоры, или открыто сексуальные беседы, а в дальнейшем даже договаривались о личной встрече…

Неконтролируемые покупки.

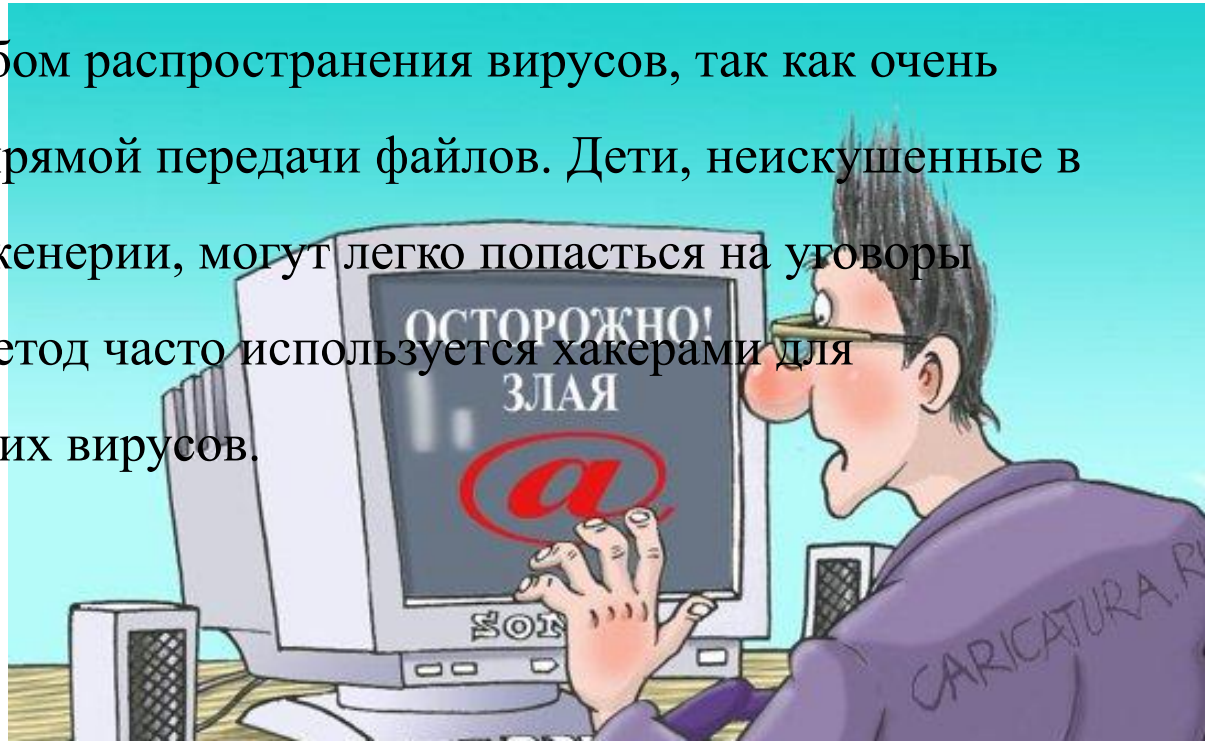
. Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.



Если Ваши дети имеют доступ к Вашим банковским данным или номеру кредитной карты, они могут приобрести практически что угодно через Интернет, от постера до роскошной машины, или оплатить услуги, варьирующиеся от онлайновых игр до путешествия вокруг света.

Угроза заражения вредоносным ПО.

Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.



опасности, с которыми мы можем столкнуться в сети

Доступ к неподходящей информации:

- **сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;**
- **сайты, размещающие изображения порнографического или иного неприемлемого сексуального контента, к которым дети могут легко получить доступ;**
- **сайты с рекламой табака и алкоголя;**
- **сайты, посвященные изготовлению взрывчатых веществ;**
- **сайты, пропагандирующие наркотики;**
- **сайты, пропагандирующие насилие и нетерпимость;**
- **сайты, публикующие дезинформацию;**
- **сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;**
- **сайты, позволяющие детям принимать участие в азартных играх онлайн;**
- **сайты, на которых могут собирать и продавать частную информацию о Ваших детях и Вашей семье.**

О чем кричит статистика

Десять правил безопасности для детей в Интернете*

1. Посещайте сеть вместе с детьми, поощряйте их делиться опытом использования Интернета
2. Научите детей доверять интуиции - если их в Интернете что-либо беспокоит, пусть сообщают вам
3. Помогите ребенку зарегистрироваться в программах, требующих регистрационного имени и заполнения форм, не используя личной информации (имя ребенка, адрес электронной почты, номер телефона, домашний адрес). Для этого можно завести специальный адрес электронной почты

4. Настаивайте, чтобы дети никогда не давали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки
5. Объясните детям, что в Интернете и реальной жизни разница между правильным и неправильным одинакова

6. Детям никогда не следует встречаться с друзьями из Интернета, так как эти люди могут оказаться совсем не теми, за кого себя выдают
7. Скажите детям, что далеко не все, что они читают или видят в Интернете, - правда, приучите их спрашивать вас, если они не уверены
8. Контролируйте действия детей с помощью современных программ, которые отфильтруют вредное содержимое, помогут выяснить, какие сайты посещает ребенок и что он там делает

9. Настаивайте, чтобы дети уважали чужую собственность, расскажите, что незаконное копирование музыки, компьютерных игр и других программ - кража
10. Научите детей уважать других, убедитесь, что они знают о том, что правила хорошего тона действуют везде - даже в виртуальном мире


СОВЕТЫ ДЛЯ ДЕТЕЙ
iPad

1. Не нажимайте на ссылки. Когда Вы общаетесь в чате с помощью систем обмена мгновенными сообщениями или если Вы получили письмо, никогда не нажимайте непосредственно на ссылку, особенно если она пришла от неизвестного Вам человека.

2. Не скачивайте и не открывайте файлы из подозрительных источников.

3. Не общайтесь с незнакомцами. Пользуясь чатами и системами обмена мгновенными сообщениями, Вы никогда не знаете, с кем Вы общаетесь на самом деле.

4. Не распространяйте через Интернет свою конфиденциальную информацию. Никогда не отправляйте личную информацию (Ваши данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуйте такого рода информацию в блогах и форумах.

5. Будьте бдительны. Если программа, которую Вы не помните, чтобы устанавливали, начинает показывать Вам всплывающие окна с предложением что-то купить, будьте бдительны.

6. Не запускайте подозрительные файлы. Если Ваше решение безопасности скажет Вам, что файл может содержать (или содержит) вредоносную программу, не открывайте этот файл. Просто удалите его.

7. Поговорите с Вашими родителями или учителями. Если у Вас возникли вопросы обо всем этом, если Вы столкнулись с чем-то подозрительным, если Вы получили оскорбительные или опасные письма, то обсудите это с взрослыми. Они смогут Вам помочь.

НЕ ЗАБЫВАЕМ О ИНТЕРНЕТ ЭТИКЕ

Не делайте ваши письма длиннее, чем они должны быть. У каждой мысли есть начало и конец. Да и 15-20 слов в одном предложении электронного послания – именно та норма, которую получатель e-mail, а может воспринимать в Интернете без напряжения для глаз и психики.

Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.

Опытные пользователи также вносят шаблонные приветствия и благодарности, которые вставляются в начало или конец каждого послания, в награду «за уделенное время». Так что даже в Интернете не стоит пренебрегать этикетом, вне зависимости о темы переписки. Ведь электронное послание лишь создается в Сети – прочитает его, все равно, живой человек

БЕЗОПАСНАЯ РАБОТА В СЕТИ

1. Не ходите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

3. Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов.

5. Никогда, никому не посылайте свой пароль.

6. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше сгенерите его специальной программой или попросите сделать это своего провайдера.

СПАСИБО ЗА ВНИМАНИЕ