

Распространенные опасности в Интернете и правила безопасности





на шаг впереди

...риски и опасности

Технологические
(вредоносное ПО, СПАМ,
хищение ПД)

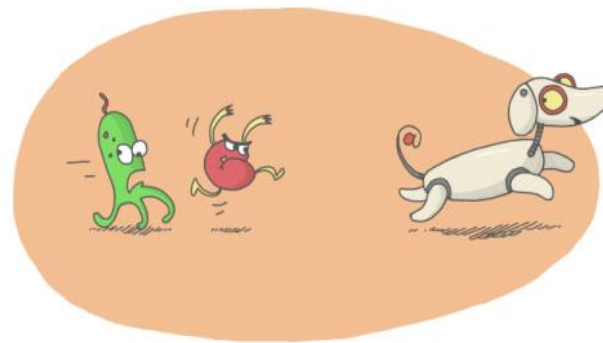
Коммуникационные
(домогательство, груминг,
кибер-буллинг)

Контентные
(незаконные, неэтичные)

Потребительские
(фишинг, контрафакт,
хищения денежных средств)



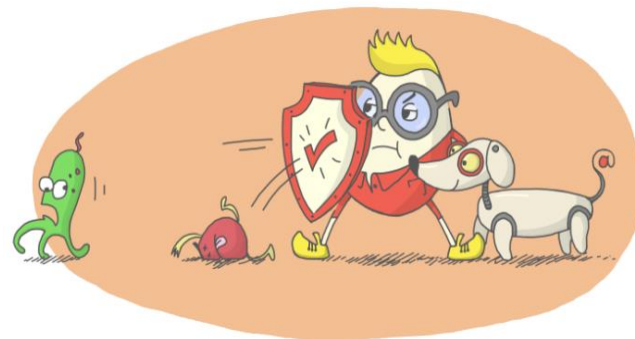
МТС предоставляет возможности по защите детей



Технологии и сервисы



Популяризация полезного
и безопасного Интернета





на шаг впереди

Распространенные опасности в Интернете и правила безопасности

Вирус и вредоносные

ОН ЗАБОЛЕЛ...?



Вредоносная программа, созданная специально для стирания, блокирования, изменения или копирования информации на компьютере против воли его хозяина.

ТРОЯНЫ

ЛОКАЛЬНЫЙ
ВИРУС

СЕТЕВОЙ
ВИРУС





на шаг вперед

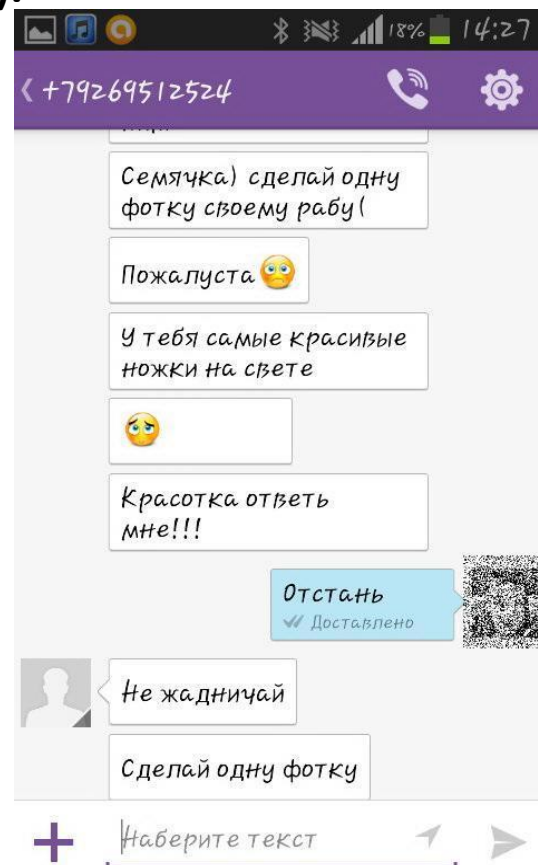
Распространенные опасности в Интернете и правила безопасности

Груминг

Это действия Интернет-хищников по поиску и завлечению своих жертв через Интернет, иные средства связи (мобильный телефон).

Правила безопасности:

- Виртуальный друг должен так и оставаться «виртуальным»;
- На встречи с интернет-друзьями нужно ходить с ребенком;
- В случае предложения выполнить неприличные действия – прервать общение ;





на шаг вперед

Распространенные опасности в Интернете и правила безопасности

Линкбомбинг

англ. *Link bomb* – «бомбежка ссылками», Хакерская шутка.

Хакер подменяет запрос в поисковике тем результатом, который ему нужен, и первым в списке может выходить интересный ему сайт – или сайт, которому он хочет отомстить.

Правила безопасности:

- Источник такой ссылки можно узнать, используя функции поисковых систем. Например, если нужный запрос в кавычках в Яндексе, поисковик выдаст всех пользователей, кто использовал именно это слово или фразу;
- Установите на компьютер антивирусные программы и фильтры, научите ребенка не доверять подозрительным ссылкам





на шаг впереди

Распространенные опасности в Интернете и правила безопасности

Контентные риски

англ. content - содержание, контент, содержимое, наполнение. Это та, информация, которую сайт доносит до нас.

Современные сайты содержат различную информацию, не всегда вся она необходима и полезна ребенку, так контентны встречаются:

- Противозаконные
- Неэтичные
- Вредоносные

Правила безопасности:

- Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
- Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
- Спрашивайте ребенка о том, что он видел и делал в Интернете, объясняйте ему «что такое хорошо, а что такое плохо».
- Обязательно научите его пользоваться линией помощи Линии помощи «Дети онлайн» (8-800-25-000-15).



Кибербуллинг

От англ. cyberbullying – преследование и унижение кого-то в Интернете или по мобильному телефону. Ребенок может столкнуться в сети с проявлением различного сетевого хамства: троллинг; прямые оскорбления; конфликтное общение в чатах.

Правила безопасности:

- Не публиковать открыто свои контакты;
- Не выкладывайте фотографии к которым легко подобрать издевательский комментарий;
- Не рассказывайте незнакомцам свою биографию;
- Блокировка «нехороших» пользователей;
- Сообщение администрации сайта или написание заявления в полицию;
- Научите делиться со взрослыми такой неприятной информацией;
- Удалить сцены унижения можно, обратившись на горячую линию (например, www.saferunet.ru)





на шаг впереди

Распространенные опасности в Интернете и правила безопасности

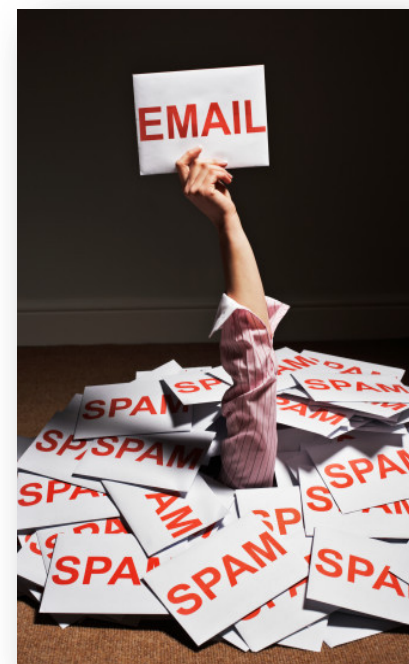
Спам

От англ. *spiced ham* – ветчина со специями.



Правила безопасности:

- Научите не оставлять почтовый ящик (телефон) в Сети или ином открытом доступе;
- Научите писать о себе телефон или e-mail только буквами «**Вася-собака-мэил-точка-ру**»;
- Настройте ребенку его почтовую программу или мобильный телефон с использованием спам-фильтров, например, Спамооборона;





на шаг вперед

Распространенные опасности в Интернете и правила безопасности

Социальные сети



Правила безопасности:

- Научите ребенка разумно размещать информацию в соц.сети;
- Научите устанавливать статус приватности личной страницы;
- Научите правилам поведения;
- Научите пользоваться «антивирусом» и проверять все присылаемые «приложения»;
- Не разрешайте тратить деньги в сети (игры на деньги и.т.п);
- Горячая линия: «Дети онлайн» 8 (800) 25-000-15 или отправить электронное письмо на адрес: helpline@detionline.com



на шаг впереди

Распространенные опасности в Интернете и правила безопасности

Фишинг

Один из видов мошенничества, когда пользователю подсовывают фальшивые веб-страницы или сообщения от банков или платежных сервисов.

Правила безопасности:

- Расскажите о том, какие случаи мошенничества встречаются на сайтах.
- Убедитесь в безопасности сайта, на котором вы или ваш ребенок планируете совершить покупку.
- Не оставляйте в свободном доступе для ребенка банковские карты и платежные данные, с помощью которых он может совершить покупку самостоятельно.





на шаг вперед

Распространенные опасности в Интернете и правила безопасности

Цифровой наркотик

Название для звуковых файлов, предположительно вызывающих психоактивное действие. Само явление появилось вместе с программой I-Doser в середине 2006 года, а в 2009 году испытало всплеск популярности в интернете.

Правила безопасности:

Сейчас продажей «ЦН» занимаются только мошенники. Они хотят продать обычную музыку за большие деньги как «необычную», называя её по имени реальных наркотиков. При этом за каждый файл необходимо отправить «недорогую» смс, реальная стоимость которой может достигать тысячи рублей. Доверчивому пользователю пишут на сайте стоимость СМС-ки из расчета за один день, в том время как деньги с телефона списываются сразу **за 3 мес.**





на шаг впереди

Распространенные опасности в Интернете и правила безопасности

Доменные махинации

англ. *domain* - область, поле деятельности. Это то, что мы привыкли считать адресом сайта.

Правила безопасности:

- При посещении неизвестного сайта обратите внимание на его правильное написание;
- Для того, что бы защититься от подобной махинации достаточно использовать **фильтр для браузера**.



Угрозы для детей в Интернете

Ежедневно дети и подростки сталкиваются с целым рядом сетевых рисков

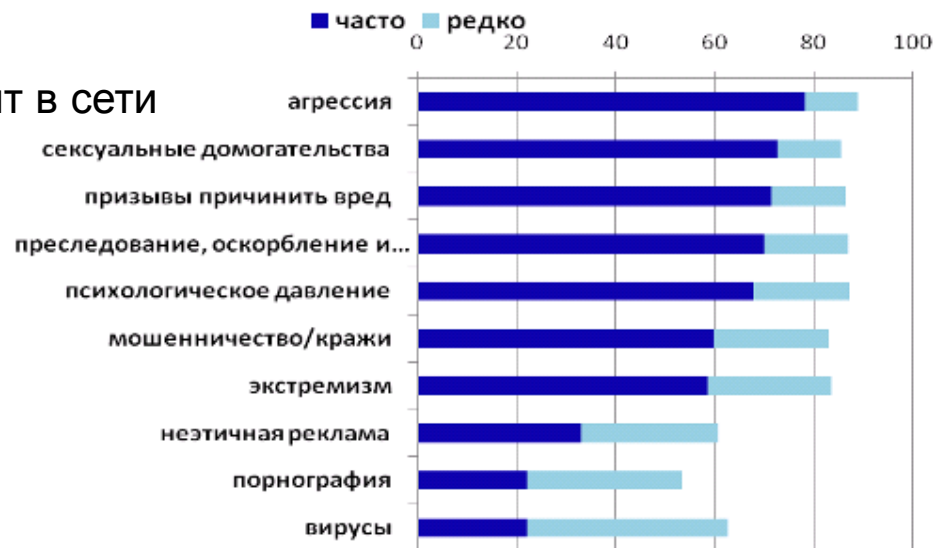
- Почти половина детей проводит в интернете 1-3 часа ежедневно
- Каждый десятый ребенок проводит в сети 5-10 часов в день

Контентные риски:

- непредназначенный для детей (неподобающий) контент
- незаконный контент

Электронная безопасность:

- вредоносные программы (вирусы, рекламное, шпионское ПО и т.п.)
- кибермошенничество
- спам



- 78% детей часто сталкиваются в интернете с агрессией.
- Более 2/3 старшеклассников часто сталкиваются с сексуальными домогательствами, призывами причинить себе вред, преследованиями, оскорблениями и психологическим давлением.
- Больше половины детей сталкиваются с мошенничеством и экстремизмом.
- Каждый пятый – с неэтичной рекламой, порнографией и вирусами.



на шаг вперед

Другие полезные ресурсы для детей и родителей

Полезная информация о технологиях детской безопасности в Интернете:

- Справочник по детской безопасности в Интернете: www.google.ru/goodtoknow/
- Фонд развития Интернет www.fid.ru
- Понятный Интернет www.zaprosto-internet.ru
- 10 шагов в Интернете www.google.ru/intl/ru/landing/internetsovety/
- Образовательный проект «Дети в Интернете» www.detionline.com/mts/lessons
- Национальный детский фонд www.ndfond.ru
- Смешарики www.smeshariki.ru
- Онлайн игра «Изучи Интернет – управляй им» www.igra-internet.ru
- Твиди www.tvidi.ru (6-16 лет)
- ЮНИСЕФ (межд. организация представлена более, чем в 150 странах мира). Защита прав детей и другие направления www.unicef.ru
- Центр безопасного Интернета в России www.saferunet.ru

