

Интернет – это часть ежедневной жизни наших детей. Они часами подключены к Интернету, находясь дома или в школе. Именно поэтому родители и дети должны быть осведомлены о рисках в Интернете, а также должны знать о том, как их можно избежать.

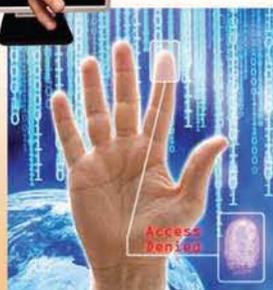
Согласно данным Save the Children, свыше 13 миллионов детей в Европе регулярно пользуются Интернетом: четыре миллиона детей в возрасте до 12 лет и девять миллионов детей в возрасте от 12 до 17 лет.



## РЕБЕНОК В СЕТИ

### Основные источники РИСКА

Системы обмена мгновенными сообщениями стали широко используемым каналом общения для молодых людей и оружием в руках кибер-преступников для организации своих атак.



## МГНОВЕННЫЕ СООБЩЕНИЯ

1. Одна из главных опасностей – **ОБМАН**: общаться с детьми от лица других людей. Эта тактика часто используется педофилами. Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайн, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.



2. **ЗАРАЖЕНИЕ ВИРУСАМИ.** Следуйте простому совету: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через Интернет. Не делайте этого, если не убедитесь, что получили от действительно знакомого человека.

## ПОЧТА

В этом случае также существует две угрозы:

1. **СПАМ.** Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств.



**ДЕТИ БОЛЕЕ НАИВНЫ, ЧЕМ ВЗРОСЛЫЕ, И МОГУТ ВЕРИТЬ ВСЕМУ, ЧТО ОНИ ПРОЧИТАЛИ В ПИСЬМАХ.** Они могут начать играть в азартные игры или покупать опасные лекарства и даже наркотики.



2. **ЗАРАЖЕНИЕ ВИРУСАМИ.** Некоторые письма имеют привлекательные темы, заставляющие пользователей нажимать ссылки и скачивать файлы (которые потом являются причиной заражения): реклама новых фильмов, эротические фотографии, скачивание игр и т.д. Многие взрослые люди становятся жертвами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.



## ОБМЕН ФАЙЛАМИ

Обмен файлами через такие программы как Emule или Kazaa является самым распространенным способом заражения компьютеров. Многие вирусы и угрозы используют названия фильмов, программ и т.д., чтобы побудить пользователя скачать их и открыть.

**ДЕТИ ДОЛЖНЫ ЗНАТЬ, КАКИЕ ФАЙЛЫ ОНИ МОГУТ СКАЧИВАТЬ, А КАКИЕ – НЕТ.**



**СОТОВЫЕ ТЕЛЕФОНЫ – НОВЫЕ СРЕДСТВА ОБЩЕНИЯ С ТАКИМИ ЖЕ РИСКАМИ, КАК И В ИНТЕРНЕТЕ**



## СОЦИАЛЬНЫЕ СЕТИ И БЛОГИ

Социальные сети для обмена файлами, знакомства с людьми и др., а также блоги стали одними из самых популярных ресурсов среди молодежи. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д. Как правило, достаточно только указать адрес электронной почты и имя, которое может быть псевдонимом или ником. **НЕЛЬЗЯ РАСПРОСТРАНЯТЬ ТАКУЮ ИНФОРМАЦИЮ, КАК ВОЗРАСТ, АДРЕС ПРОЖИВАНИЯ, А ТАКЖЕ СВОИ ФОТОГРАФИИ И ВИДЕО.**





## СОВЕТЫ ДЛЯ РОДИТЕЛЕЙ

**1 Поговорите с вашими детьми.** Вы должны знать, какие сайты они посещают, с кем они общаются, что они любят смотреть и т.д. Вы не должны позволять им уходить из дома и не предупреждать Вас, куда и с кем они пошли. Соответственно, Вы не должны разрешать им пользоваться Интернетом, если они не знают, как с ним обращаться.

**2 Обучите себя и поделитесь этими знаниями с вашими детьми.** Для многих родителей Интернет является все еще неизвестным миром. По этой причине очень важно знать о тех утилитах, которые Интернет предлагает детям, о рисках, которые они могут в себе нести, а также о том, как их можно избежать.

**3 Установите правила для использования Интернета.** Вы должны установить четкие и понятные правила, которые описывают расписание выхода в Интернет, максимальную продолжительность работы в Интернете, а также способ его использования. Убедитесь, что Ваши дети следуют этим правилам, особенно при использовании Интернета ночью. Если у Вас только один ПК на всю семью, то он должен располагаться в общей комнате, а не в спальне Вашего ребенка.

**4 Запретите детям предоставлять конфиденциальную информацию.** Вы должны проинструктировать Ваших детей о том, что им нельзя предоставлять кому-либо в Интернете такие данные, как их имя, адрес или свои фотографии. Посоветуйте им использовать псевдоним или ник.

**5 Научите своих детей быть осторожными.** Информация в Интернете может быть обманчивой. Научите Ваших детей быть осторожными и приучить их не делать ничего такого, что могло бы поставить под угрозу их безопасность и конфиденциальность.

**6 Установите эффективное решение безопасности.** Чтобы защитить Ваших детей от вредоносных программ, лучший способ – это использовать обновляемое и эффективное решение безопасности, например, PANDA.

# PANDA

SECURITY

# РЕБЕНОК В СЕТИ



# РЕБЕНОК ИГРАЕТ?

ПОДРОБНОЕ РУКОВОДСТВО  
ПОМОЖЕТ ОБЕСПЕЧИТЬ  
БЕЗОПАСНОСТЬ ВАШИХ ДЕТЕЙ  
В ИНТЕРНЕТЕ

