Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Риски
- Обучение детей

# Правила компьютерной безопасности для детей

## Обзор

В современном мире у детей есть поразительные возможности выходить в сеть и общаться онлайн. Новые социальные сети возникают неожиданно, и количество приложений и онлайн игр постоянно растет. Кроме того, многие школы перешли к использованию сервисов, подобных Google Drive и требуют выполнения всех или некоторых заданий онлайн. Дети, образно говоря, растут «в сети». В этом есть свои преимущества и недостатки. В этом выпуске мы поговорим о трёх основных областях риска и о том, как помочь детям обеспечить безопасность.


### Об авторе

Боб Рудис - исследователь безопасности данных в компании Verizon, автор Data Breach Investigations Report 2015 и наставник четырёх замечательных детей. Боб создал и проводил множество увлекательных и эффективных программ обучения безопасности в компаниях из списка Fortune 100. Боб ведёт блог в Twitter как **@hrbrmstr**.


## Риски

1. **Поведение**: Общаясь в виртуальном пространстве или онлайн сообществе, дети могут вести себя так, как никогда не будут в реальности. Физическое отсутствие дает ощущение анонимности, особенно у детей. Поэтому они часто утверждаются за счёт унижения других, так называемое онлайн запугивание или интернет хулиганство. Есть вероятность, что ваши дети могут стать жертвой других детей, которые попытаются им навредить.

2. **Контактная информация**: Современные дети постоянно находятся на связи с другими, будь то смс сообщения, общение в социальных сетях или онлайн игры. Физическое отсутствие снижает бдительность, и они забывают, что на другой стороне может быть совсем не тот человек, которым представляется незнакомец и у него не всегда добрые намерения. Хищники бродят по онлайн каналам, и они сделают все возможное, чтобы выстроить отношения с потенциальными жертвами, даже выдают себя за детей, чтобы наладить контакт.

3. **Содержание**: Существует огромное количество способов перехвата и публикации текстовых, голосовых или видео сообщений в Интернете. Зачастую дети не видят реальной опасности в публикации информации о себе или членах своей семьи. Также дети не видят опасности в просьбах ответить на вопросы или

# Правила компьютерной безопасности для детей

переходе по ссылке, которые приводят к краже личных данных или заражению компьютера вирусами. Наконец, мы живем в то время, когда нельзя «отменить» информацию, размещённую в сети, или переданную другим людям. Дети думают, что сообщения в Kik, Instagram, Snapchat или других сервисах мимолётны, но они могут всплыть позже и преследовать их или их семью в дальнейшей жизни.

*Лучший способ защиты детей – научить их видеть опасности и объяснить, что не только вы с ними говорите, но и они всегда могут к вам обратиться.*

## Обучение детей

Самое простое, что вы можете сделать для защиты детей, просто поговорить с ними. Узнайте, что ваши дети делают онлайн и расскажите о современных опасностях и способах защиты от них.

1. **Безопасность дома**: Даже учитывая современную мобильность, дом – это то место, где формируются навыки безопасного поведения в сети. Чем раньше вы будете говорить с детьми, а они с вами, тем лучше. Регулярно рассказывайте об онлайн опасностях и их последствиях. Если вы не знаете, чем ваши дети занимаются, просто спросите у них. Притворитесь невежественным родителем и попросите объяснить, как они пользуются некоторыми современными технологиями. Детям нравится роль учителя, и они откроются. Например, если они общаются в Instagram, попросите показать, как работает этот сервис, создать вам аккаунт и отслеживайте с его помощью их деятельность. Вы не только сможете отслеживать своего ребенка, но и упростите ваше с ним общение. В дополнение к этому, вы можете создать в доме территорию для онлайн общения и ввести временные ограничения. Используя компьютер на такой территории у ребёнка меньше шансов нарваться на неприятности. Ещё одна хорошая идея – централизованное место зарядки мобильных устройств, в котором следует оставлять их на ночь.

2. **Безопасность вне дома**: Вне дома дети подвержены большему риску. Объясните, что правила онлайн безопасности действуют везде и объясните это тому, кто за ними присматривает. Если у них есть мобильное устройство, проверяйте его историю (время и объём данных, переданных в интернет) чтобы отследить нарушения правил безопасности. Вы не можете оградить детей от всего, но они могут вспомнить ваши заботливые наставления во время онлайн активностей.

3. **Безопасность в числах**: Вы не одиноки в своем желании обезопасить ребёнка, поэтому следует вовлекать в этот процесс других родителей, опекунов, родственников, учителей и друзей. Это поможет

# Правила компьютерной безопасности для детей

отследить потенциально опасное поведение. Постарайтесь, чтобы ваш круг общения в доброжелательной форме предостерегал ребёнка от опасных действий.

Наконец, ошибки детей нужно воспринимать как опыт, а не повод для наказания. Всё время объясняйте «почему» и напоминайте, что вы всего лишь пытаетесь их защитить от потенциальной опасности. Пусть знают, что всегда могут с вами обсудить любые сомнения по поводу онлайн общения и даже показать вам скриншот. Убедитесь, что они понимают, что всегда могут обратиться к вам за помощью, даже если совершили что-то неуместное. Создание условий для открытого и активного общения – лучший способ помочь детям обеспечить безопасность в современном онлайн мире.

## Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом. Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

## Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

## Ресурсы

| | |
|---|---|
| Cyber Smart: | http://www.cybersmart.gov.au/Parents.aspx |
| OnGuard Online: | http://www.onguardonline.gov/topics/protect-kids-online |
| Stay Safe Online: | https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens |
| Securing Kids Panel: | |
| http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace | |
| Дети в интернете: Опасности реальны: | http://nedopusti.ru/articles/read/85/ |
| В чем опасность интернета для детей?: | http://bezopasnost-detej.ru/kak-zashchitit-rebenka/72-opasnost-interneta-dlya-detej |



Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова



 