Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Три основные опасности
- Защита ваших детей
- Ресурсы

Защита детей от онлайн опасностей

ОБ АВТОРЕ

Автор этого выпуска OUCH – Кевин Джонсон. Кевин является президентом фирмы **Secure Ideas**, отвечает за выпуск сайта MySecurityScanner.com. Он является старшим инструктором института SANS. Больше информации о Кевине можно найти на сайте www.secureideas.com.

ОБЗОР

Мы желаем обеспечить наших детей всем, включая возможность использовать современные технологии. Но вместе с технологиями приходят и угрозы, с которыми наши дети не могут справиться или не знают как. Наш родительский долг рассказать детям об опасностях и способах защиты, но нам это не всегда легко, так как мы выросли в другой среде. В этой статье мы поговорим о трёх основных интернет-опасностях, и способах защиты ваших детей.

ТРИ ОСНОВНЫЕ ОПАСНОСТИ

Для защиты детей, прежде всего, нужно рассказать об опасностях, с которыми они могут столкнуться в интернете.

- **Незнакомцы**: О них, прежде всего, стоит помнить родителям и защитить детей от этой онлайн угрозы. Под незнакомцами в этом контексте подразумеваются личности (чаще всего взрослые), которые налаживают онлайн контакты с детьми, чтобы воспользоваться ими, например, сексуально домогаться. Чаще всего эти люди выдают себя за детей.
- **Друзья:** Это люди, которых дети знают, чаще всего школьные друзья. Друзья могут представлять серьёзную угрозу, хулиганя онлайн. Помните, издевательства могут быть не только физическими. На самом деле Интернет усугубляет ситуацию: хулиганы могут публиковать компрометирующие сообщения на весь мир или использовать его онлайн профиль. Кроме этого, хулиганы могут совершать анонимные атаки, которые сложней отследить и прекратить. Наконец, анонимность облегчает возможность хулиганства тем, что вероятность наказания ниже.
- **Сами дети:** В современном мире социальных сетей дети могут стать себе злейшими врагами. Всё, что они публикуют, доступно не только для всего мира, но некоторые записи сложно или невозможно удалить. Дети не всегда понимают,

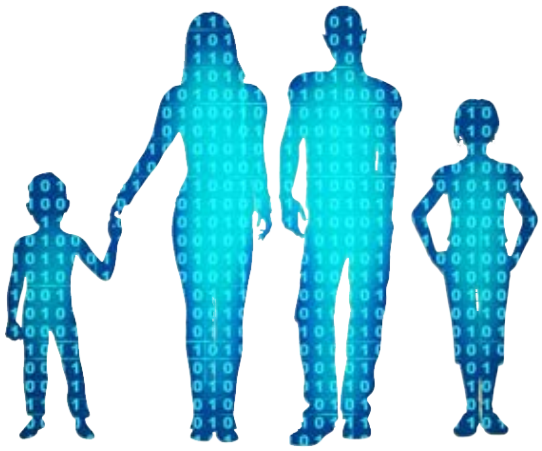
Защита детей от онлайн опасностей

как их публикации могут навредить им в будущем. Для работодателей и университетов становится обычной практикой проверять информацию о кандидате в социальных сетях и в Интернете. Вся компрометирующая или противозаконная публикация о детях или на их странице может негативно сказаться в будущем. Кроме того, личными данными могут воспользоваться незнакомцы или даже друзья во вред ребёнку или его семье.

ЗАЩИТА ДЕТЕЙ

Теперь, зная об основных опасностях, вы можете предпринять для защиты детей следующие шаги.

- **Обучение:** Самым важным шагом является обучение. Убедитесь, что дети знают об опасностях, что вы обсуждаете с ними их онлайн действия, и вы знаете о том, что они делают в сети. Кроме этого, создайте благоприятную атмосферу, чтобы ребёнок всегда делился проблемами и обращался с вопросами, возникающими онлайн.
- **Отдельный компьютер:** По возможности, обеспечьте ребёнка отдельным компьютером. Если ребёнок случайно заразит свой компьютер, то ваши аккаунты, например, онлайн банкинг, будут в безопасности. Кроме этого, установите детский компьютер в открытой зоне, чтобы видеть их онлайн активность. Наконец, убедитесь, что каждый ребёнок пользуется личным аккаунтом без прав администратора. Это даст возможность отслеживать действия каждого ребёнка.
- **Мобильные устройства:** С мобильными устройствами ситуация сложнее. Следует установить сроки, когда дети могут ими пользоваться, а в



Лучшая защита ваших детей в интернете - рассказать о возможных рисках. Установите правила, определяющие, что можно делать в интернете, а чего делать нельзя.

остальное время возвращать устройства вам (например, создайте семейный центр подзарядки). Также забирайте устройства на ночь, чтобы дети вместо сна не сидели в Интернете.

- **Социальные сети:** Отслеживайте действия детей в социальных сетях с помощью своего аккаунта, например в Facebook, Twitter или Instagram, добавьте ребенка в друзья, так вы сможете видеть все его публикации.
- **Правила:** Создайте документ с правилами, которым дети должны следовать онлайн. В правилах следует оговорить время пользования сетью, длительность, какие игры и приложения можно использовать, какие нет, какую информацию можно публиковать, а какую нет. Кроме этого, следует рассказать, как правила должны соблюдаться и какие наказания

Защита детей от онлайн опасностей

предусмотрены за нарушения. Ознакомьте детей с документом и сохраните его на их компьютере, чтобы дети знали, что вы от них ожидаете.

- **Технологии:** Наконец, существуют современные технологии, с помощью которых можно фильтровать и контролировать деятельность детей в Интернет. В большинстве операционных систем есть функция родительского контроля, есть дополнительные бесплатные и коммерческие инструменты, например, OpenDNS. Эти технологии безопасности работают с маленькими детьми. Чем старше дети, тем технологии менее эффективны. Кроме того, что старшие дети нуждаются в расширенном доступе к ресурсам для учёбы или работы, у них есть устройства, которые вы не можете контролировать, например, компьютер в библиотеке или компьютер родственника, друга. Кроме того, в программном обеспечении некоторых мобильных устройств отсутствует функция родительского контроля, например, iPad и iPhone. Вот почему обучение и правила поведения в сети гораздо эффективнее, чем отдельные технологии.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

6 советов, которые помогут обеспечить безопасность в Интернете:
http://tinyurl.com/dxq6sak

Онлайн безопасность для детей:
http://preview.tinyurl.com/3s5augb

Как обеспечить безопасность детей в Интернете:
http://preview.tinyurl.com/bszx3et

Безопасность детей в Интернете:
http://preview.tinyurl.com/chhdw2a

Сайт для родителей «Безопасность детей в интернете»:
http://ikeepsafe.org/PRC

Сервис OpenDNS:
http://preview.tinyurl.com/3m37k3k

Термины по информационной безопасности:
http://preview.tinyurl.com/6wkpae5

Ежедневные советы Института SANS по информационной безопасности:
http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков