

Безопасный интернет



Правило 1

Ни за что не раскрывай свои личные данные. Бывает так, что сайт требует ввода твоего имени. В этом случае просто необходимо придумать себе псевдоним (другое имя). Никогда не заполняй строчки, где требуется ввести свою личную информацию: адрес, фамилию, дату рождения, телефон, фамилии и имена друзей, их координаты ведь просмотреть их может каждый. А этого вполне достаточно для того, чтобы узнать о твоей семье и уровне вашего благосостояния. Этим могут воспользоваться воры и мошенники не только в виртуальной, но и реальной жизни.



Правило 2

Если ты вдруг хочешь встретиться с «интернет-другом» в реальной жизни – обязательно сообщи об этом родителям. Не всегда бывает так, что «друзья» в интернете, нам знакомы в реальной жизни. И если вдруг твой новый знакомый предлагает тебе встретиться, посоветуйся с родителями. В интернете человек может быть совсем не тем, за кого себя выдаёт, и в итоге якобы двенадцатилетняя девочка оказывается сорокалетним дядечкой, который может тебя обидеть.



Правило 3

Старайся посещать только те страницы интернета, которые тебе советуют родители. Они – люди взрослые и лучше знают, что такое хорошо и что такое плохо. А, кроме того, они нас очень любят и никогда плохого не посоветуют. Нам часто хочется взрослости и самостоятельности. Не упрямясь!



Правило 4

В сети ты можешь оказаться на вредных страницах с совсем не детским содержанием. Расскажи об этом родителям, если тебя что-то встревожило или смутило. Практически любой «клик» по интересной, нужной или полезной ссылке может привести к переходу на сайт, предлагающий бесплатно скачивать и просматривать «взрослые страницы».



Правило 5

Никогда без ведома взрослых не отправляй СМС, чтобы получить информацию из интернета. Иногда всплывает окошко – очень яркое, даже мигающее, примерно с такими словами: «Только сегодня – уникальный шанс –

участвуй и выигрывай!» Заманчиво, правда? Ты щёлкаешь на него и тут сообщение: «Для того, чтобы принять участие в розыгрыше тебе необходимо прислать СМС!» Остановись! Ни в коем случае не делай этого без ведома взрослых, ведь это могут быть мошенники. И одна, казалось бы, безобидная СМС-ка может стоить тебе больших денег.



Не забывай, что интернет – это не главное увлечение в жизни. Кроме него у тебя должны быть любимые книги, занятия спортом и прогулки с друзьями на свежем воздухе!

Сетевичок.рф - обучение и онлайн-консультирование по вопросам кибербезопасности

Дорогие студенты, в помощь вам создан сайт специально для подростков. В любое время вы можете зайти на этот сайт и получить ответы на многие вопросы.

Сайт «Сетевичок» является центром поддержки подростков в киберпространстве и обучения основам кибербезопасности. Эксперты сайта помогут решить проблемы, окажут содействие в критической ситуации, дадут консультацию. На сайте можно пройти обучение по кибербезопасности и узнать основные методы киберзащиты.



Какие угрозы встречаются наиболее часто? Прежде всего:

● **Угроза заражения вредоносным ПО.** Ведь 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.

● **Доступ к нежелательному контенту.** Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые

материалы. А это насилие, наркотики порнография, страницы, подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера.

● **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.

● **Неконтролируемые покупки.** Несмотря 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.

Интернет — это прекрасное место для общения, обучения и отдыха. Но стоит понимать, что наш реальный мир, всемирная паутина так же может быть весьма и весьма опасна.