

БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ



Содержание

1

Опасности, с которыми дети могут столкнуться в Сети

2

Безопасное общение детей в Интернете

3

Профилактика Интернет-зависимости у учащихся

4

Технологии безопасной работы в сети

Угрозы сети Интернет

- **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. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.



- **Неконтролируемые покупки.** Не смотря 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.

Угрозы сети Интернет

► Угроза заражения вредоносным ПО.

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.



Угрозы сети Интернет

Множество вебсайтов, электронных сообщений или программ обмена файлами позволяют пользователям скачивать все виды музыки, игр, документов и т.д. Однако, несмотря на их кажущуюся безобидность, многие из них содержат вирусы.



Общие правила безопасности при работе в Интернете:

- ▶ Ребенку не следует давать частной информации о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей.

Не нужно предоставлять личную информацию через Интернет



Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность - отличный способ защиты. Не выкладывайте фотографии ребенка на веб-страницах или публичных форумах.

Общие правила безопасности при работе в Интернете:

- ▶ Не следует открывать письма электронной почты, файлы или Web-страницы, полученные от людей, которые не знакомы или не внушают доверия.



Нужно знать как поступать при столкновении с подозрительным материалом, что не нужно нажимать на ссылки в электронных сообщениях от неизвестных источников, открывать различные вложения. Такие ссылки могут вести на нежелательные сайты, или содержать вирусы, которые заразят Ваш компьютер. Удаляйте с Вашего компьютера следы информации, которую нежелательно обнаружить Вашему ребенку.

Инструкции по безопасному общению в чатах

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

Интернет-этика

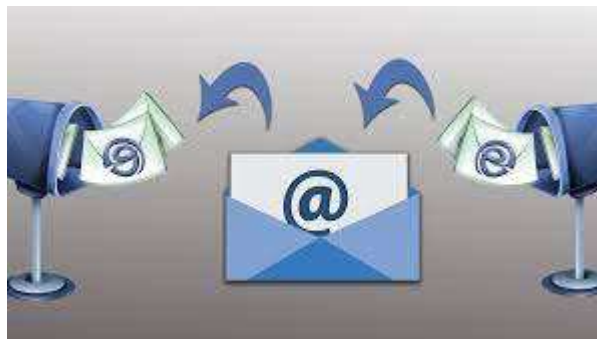


- ▶ Узнайте правила прежде, чем что-нибудь сказать или сделать.
- ▶ Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.
- ▶ Не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила. Если Вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и Вы когда-то были новичком.

Интернет-этика



- ▶ Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
- ▶ Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайн чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использовать опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.
- ▶ Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).



Профилактика Интернет-зависимости у учащихся

- ▶ Экономический аспект: неспособность и нежелание отвлечься даже на короткое время от работы в Интернете; досада и раздражение, возникающие при вынужденных отвлечениях, и навязчивые размышления об Интернете в такие периоды; стремление проводить за работой в Интернете все увеличивающиеся отрезки времени и неспособность спланировать время окончания конкретного сеанса работы; побуждение тратить на Интернет все больше денег, не останавливаясь перед влезанием в долги;
- ▶ Межличностный аспект: готовность лгать друзьям и членам семьи, преуменьшая длительность и частоту работы в Интернете, способность и склонность забывать при работе в Интернете о домашних делах и учебе, важных личных встречах, пренебрегая занятиями; стремление и способность освободиться на время работы в Интернете от ранее возникнувших чувств вины или беспомощности, от состояний тревоги или депрессии, обретение ощущения эмоционального подъема и своеобразной эйфории; нежелание принимать критику подобного рода образа жизни; готовность мириться с потерей друзей и круга общения из-за поглощенности работой в Интернете;



Профилактика Интернет-зависимости у учащихся

- ▶ аспект здоровья: резкое сокращение длительности сна; избегание физической активности, пренебрежение личной гигиеной; постоянное забывание о еде.
- ▶ За проявлениями зависимости от Интернета нередко скрываются другие аддикции, либо психические отклонения.
- ▶ Расширение симптоматики, преувеличение количества потенциальных пациентов, шума в прессе удобны на данный момент специалистам по психическому здоровью и исследователям этого феномена.



Преодоление Интернет-зависимости

1. Признайте свою зависимость. «Патологическое использование компьютера» можно распознать по «симптомам» навязчивой потребности, пропущенным урокам и встречам, забытой и несделанной домашней работе, потере контакта с друзьями и родственниками.
2. Определите проблемы, лежащие в основе зависимости. В зависимости от возраста человека, такие моменты, как неуверенность в будущем, трудность успевать в школе или проблемы социальных отношений, могут подвигнуть ребенка на побег в гостеприимные виртуальные миры.
3. Решайте реальные проблемы. Стараясь избежать стрессовых ситуаций, мы только усложняем их. Вы можете найти репетитора, который поможет с домашним заданием, поможет начать решать социальные трудности, написать о том, что вас «глохнет», или даже обратиться к специалисту.
4. Контролируйте работу на компьютере. Совсем не обязательно полностью выключать его — можно просто ограничить время нахождения в Интернете. В зависимости от возраста родители или сам учащийся могут взять на себя эту ответственность. Все виды деятельности должны быть выстроены по их приоритетности. Общение в Интернете не должно происходить до выполнения домашней работы или других обязанностей.
5. Проводите различие между интерактивной фантазией и полезным использованием Интернета.

Технологии безопасной Работы в сети

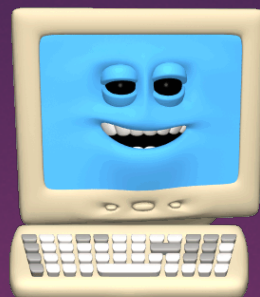
► Безопасность при навигации по сайтам и по приему почты

1. Не ходите на незнакомые сайты.
2. Если ходите, то выключайте (на всякий случай) поддержку языка Java и использование cookies.
3. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.
4. Если пришел **exe-файл**, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов.
5. Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).
6. Никогда, никому не посылайте свой пароль.
7. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше сгенерируйте его специальной программой или попросите сделать это своего провайдера.

Безопасность при работе на общедоступном компьютере

1. Не сохраняйте свои учетные данные для входа в систему.
2. Не оставляйте без присмотра компьютер с важными сведениями на экране.
- 3.Заматайте свои следы.
- 4.Опасайтесь подглядывания через плечо.
- 5.Не вводите важные сведения на общедоступном компьютере.

Безопасность в соц. сетях



СОЦИАЛЬНАЯ СЕТЬ – удобный способ общения с друзьями

легко отправлять сообщения,
смотреть и комментировать фотографии...
А если копнуть глубже?

ЗНАЕТЕ ЛИ ВЫ



ВСЮ ИНФОРМАЦИЮ, которую вы даже ограничиваете и скрываете от других, так называемых «чужих» пользователей, ВСЕ РАВНО МОЖНО УВИДЕТЬ, взломав ваш аккаунт

Скептически относитесь к распределению в сетях на друзей и
незнакомых

ПОМНИТЕ, ДОСТУП ЕСТЬ У ВСЕХ !

ВЫХОД ЕСТЬ

НЕ ДОБАВЛЯЙТЕ в друзья тех, кто
вам малоизвестный, незнаком или
подозрителен,

обезопасьте себя лишний раз,
пожертвовав возрастанием
количества друзей

ПОМНИТЕ

В СОЦИАЛЬНЫХ СЕТЯХ люди собираются НЕ
ТОЛЬКО, ЧТОБЫ ПООБЩАТЬСЯ

В интернете МАССА МОШЕННИКОВ, и тех,
которые не готовы возрадоваться вашему
счастью

Сила действия ОТРИЦАТЕЛЬНОЙ ЭНЕРГИИ и
ее РАЗРУШАЮЩИЙ ХАРАКТЕР давно
доказан учеными

СЛЕДОВАТЕЛЬНО

С АККУРАТНОСТЬЮ ВЫКЛАДЫВАЙТЕ
ФОТОГРАФИИ, на которых запечатлены
ваши дорогостоящие вещи,

ОБЕЗОПАСЬТЕ СЕБЯ ОТ ВОРОВ И
МОШЕННИКОВ

По имени и фамилии легко можно узнать
адрес, номер телефона и выследить момент,
когда вас не будет дома

НЕ АФИШИРУЙТЕ В СОЦИАЛЬНЫХ СЕТЯХ

что планируете отправиться
в путешествие или отпуск,

этой информацией

Можно воспользоваться

НЕ НА ВАШУ ПОЛЬЗУ





ДРУГАЯ ИСТОРИЯ...

**Помимо кражи и использования
личных данных в корыстных целях,
социальные сети**

играют еще и значительную роль

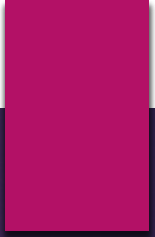
в деле распространения вирусов,
троянских программ, червей и
прочего вредоносного
программного обеспечения,

Tect



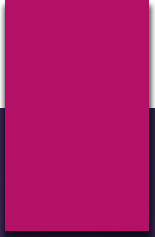
А теперь для проверки полученных знаний
необходимо ответить на некоторые вопросы
теста:

- 1) Всегда ли можно быть уверенным в том,
что электронное письмо было получено от
указанного отправителя?
 - а) Да
 - б) Да, если знаете отправителя
 - в) Нет, т.к. данные можно легко подделать



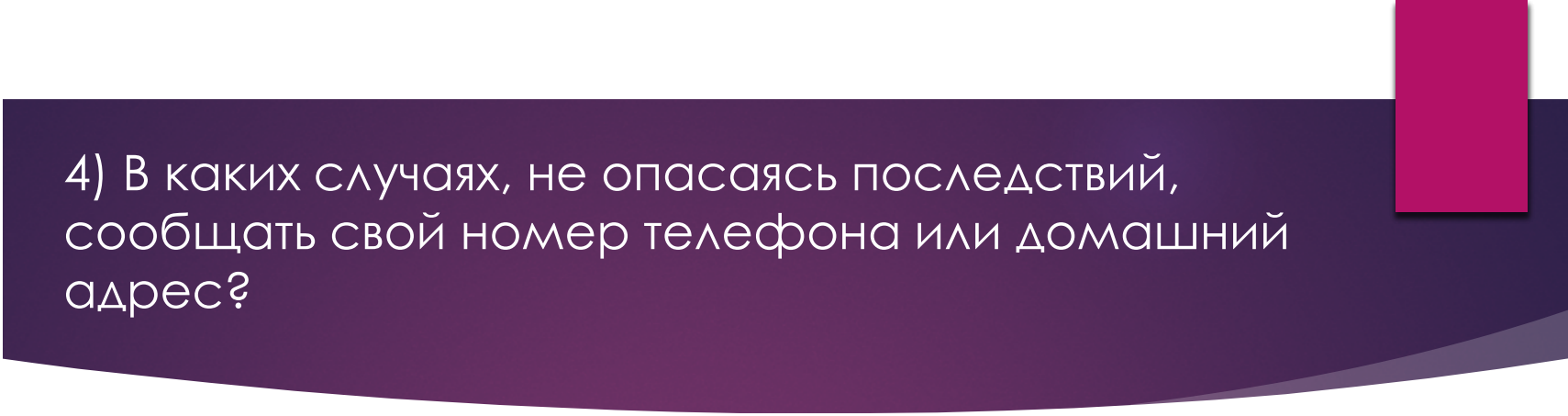
2) Что нужно сделать при получении подозрительного сообщения?

- а) Удалить его, не открывая
- б) Открыть его и выяснить, содержится ли в нем какая либо важная информация
- в) Открыть вложение, если таковое содержится в сообщении
- г) Отправить его родителям



3) Вам пришло «письмо счастья», в котором говорится чтобы вы его переслали 5 друзьям. Какие ваши действия?

- а) Переслать его пяти друзьям
- б) Переслать его не 5, а 10 друзьям
- в) Никому не пересылать
- г) Ответить отправителю, что вы не хотите больше получать подобные письма

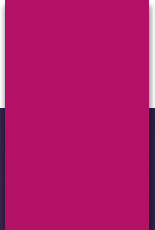


4) В каких случаях, не опасаясь последствий, сообщать свой номер телефона или домашний адрес?

- а) Во всех случаях
- б) Когда кто-то специально просит об этом
- в) Когда собеседник в чате просит об этом
- г) Такую информацию следует с осторожностью сообщать людям, которым вы доверяете

5) Что запрещено в интернете?

- а) Запугивание других людей
- б) Поиск информации
- в) Игры
- г) Общение с друзьями



**Спасибо за
внимание!**