Спецвыпуск

МБОУ «Школа № 105»

Февраль 2016 года

Стопятка

Газета для учеников, учителей и родителей

Всё будет хорошо!

9 февраля 2016 года—Всемирный день безопасного Интернета
Праздник был учреждён по инициативе Европейской комиссии в 2004 году с целью пропаганды более безопасного и ответственного использования Интернета

Рисунок Анастасии Подгорной, 9А

В ЭТОМ ВЫПУСКЕ:

Внимание! Опрос

Среди учащихся 9-х классов мы провели опрос «Безопасность в интернете». Вот как ответили ребята на наши вопросы.

1 вопрос:

Каким образом вы обеспечиваете свою безопасность в интернете?

- Выбираю безопасные пароли - 35,3%
- Не размещаю в интернете личную информацию - 41,2%
- Использую лицензионные антивирусники - 52,9%
- Сохраняю в чистоте адрес электронной почты - 5,9%
- Не отвечаю спамерам - 47,1%
- Не храню в компьютере важную информацию - 5,9%
- Запароливаю сеть Wi-Fi - 47,1%

Таким образом, многие не обращают особого внимания безопасности электронной почты и опасности взлома хакерами домашнего компьютера.

2 вопрос:

Считаете ли вы нужным выставлять свою личную информацию в социальные сети?

- Да - 5,9%
- Нет - 58,8%
- Никогда не задумывался - 35,3%

Радует, что больше половины опрошенных ответили «нет», но велик процент тех, кто вообще об этом не думает. Значит, эта тема требует разъяснения.

3 вопрос:

Всех ли своих друзей в соцсетях вы знаете лично?

- Да - 47,1%
- Нет - 52,9%
- Мне всё равно - 0%
- Главное - популярность - 0%

Вывод очевиден: многие подростки приглашают в друзья тех, кого лично не знают, тем самым подвергая себя опасности.

4 вопрос:

Ставите ли вы геотметки на фото?

- Да - 5,9%
- Нет - 94,1%
- Это глупо - 5,9%
- Это модно - 0%

Здесь мы можем быть спокойны, хотя, наверное, это просто не все умеют делать.

5 вопрос:

Знакомитесь ли вы в интернете?

- Да - 47,1%
- Нет - 52,9%

Большой процент респондентов нуждается в общении, подменяя реальное виртуальным.

6 вопрос:

Встречали вы когда-нибудь своих интернет-друзей?

- Да - 35,3%
- Нет - 58,8%
- Это опасно - 5,9%
- Часто встречаю—0%

Мы видим, что большой процент ребят встречается с интернет-друзьями, не думая о том, что это может быть опасно.

7 вопрос:

Нужна ли вам безопасность в интернете?

- Да - 94,1%
- Нет - 5,9%

Необходимость безопасного интернета очевидна.

8 вопрос:

Кто должен вас научить безопасности в интернете?

- Школа - 23,5%
- Родители - 35,3%
- Друзья - 17,6%
- Интернет - 47,1%
- Другое - 17,6%

Ребята предлагают в помощники себя, тех, кто в этом разбирается и ошибки других.

Автор и организатор опроса - Алёна Тигина, 9Б.

Правила и советы

А вот вам, ребята, и первые советы-рекомендации:

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ

СЛОЖНЫЙ ПАРОЛЬ
Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Чем сложнее пароль, тем сложнее взломать твой аккаунт. Помни, что твой пароль можешь знать только ты.

СОВЕТ ВЗРОСЛЫХ
Всегда спрашивай взрослых о непонятных вещах, которые ты встречаешь в Интернете: ты не знаешь, какой пункт выбрать, на какую кнопку нажать, как закрыть программу или окно. Они расскажут тебе, как поступить - что можно делать, а что нет.

ЛИЧНАЯ ИНФОРМАЦИЯ
Никогда не рассказывай о себе незнакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому о том, где работают твои родители и номера их телефонов. Эта информация может быть использована во вред тебе и твоим родителям.

НЕ ОТПРАВЛЯЙ СМС
Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс - не делай этого! Смс на короткие номера могут стоить несколько сотен рублей. Ты потеряешь деньги, которые мог бы потратить на что-то другое.

НЕ ЗАБУДЬ ВЫЙТИ
При использовании чужих компьютеров или мобильных устройств, не забывай выходить из своего ящика электронной почты или профилей в социальных сетях. Иначе, следующий пользователь этого устройства сможет просмотреть твою личную информацию.

ОСТОРОЖНО, НЕЗНАКОМЕЦ
Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения - сразу скажи об этом взрослым! Не все люди являются теми, за кого себя выдают в Интернете!

БЕСПЛАТНЫЙ Wi-Fi
При выходе в Интернет через общественную Wi-Fi сеть, не совершай никаких покупок и оплаты, не проверяй личную электронную почту и не передавай конфиденциальную информацию. Злоумышленники могут похитить ваши пароли и данные.

ЗАЩИТИ КОМПЬЮТЕР
Попроси родителей или сам установи систему фильтрации SkyDNS на сайте www.skydns.ru. Она защитит тебя от потери денег и кражи паролей, а также будет блокировать большую часть рекламы, ускоряя загрузку страниц в Интернете.

Безопасность в Интернете

В данной статье я бы хотела осветить актуальную в наши дни тему – «Безопасность в Интернете» и дать несколько советов о том, что можно сделать, чтобы не наткнуться на вирусы или различного рода обманы мошенников.

В наши дни почти в каждом доме имеется компьютер и другие устройства, обеспечивающие выход в Интернет. При подключении к нему пользователи подвергают свою систему различным опасностям. Одна из них – это **заражение вирусами**. В большинстве случаев, пользователь сам соединяется с зараженными машинами, когда переходит на их сайты. Даже установив на свою систему сильную защиту, нельзя быть уверенным в полной неуязвимости. Обычно бывает так: на одном из множества сайтов пользователям предлагают программу для сканирования на наличие вредоносных программ. После скачивания программы, каждый пользователь установит ее, а после запустит проверку системы. При этом заметить подвох очень тяжело, поскольку ничего особенно в скачивании и установке нет, и во время сканирования все выглядит солидно. Данная программа только выдает себя за эффективную и надежную, но она является ложным антивирусником. После проверки она показывает, что в компьютере есть вредоносные коды, и будет пытаться убедить пользователя, что они опасны. А вот здесь как раз и есть основная проблема – ведь чтобы побороть найденные «вирусы», необходимо отправить сообщение смс, либо же приобрести лицензионную программу, которая стоит совсем недешево. Как правило, здесь опытные пользователи понимают, что это обман, а наивные и доверчивые люди отдают свои деньги мошенникам, даже не думая об обмане.

Таким образом можно не только потерять свои деньги, а также запустить в свой компьютер троянскую программу (прим. программы, которые забирает всю конфиденциальную информацию) Удалить

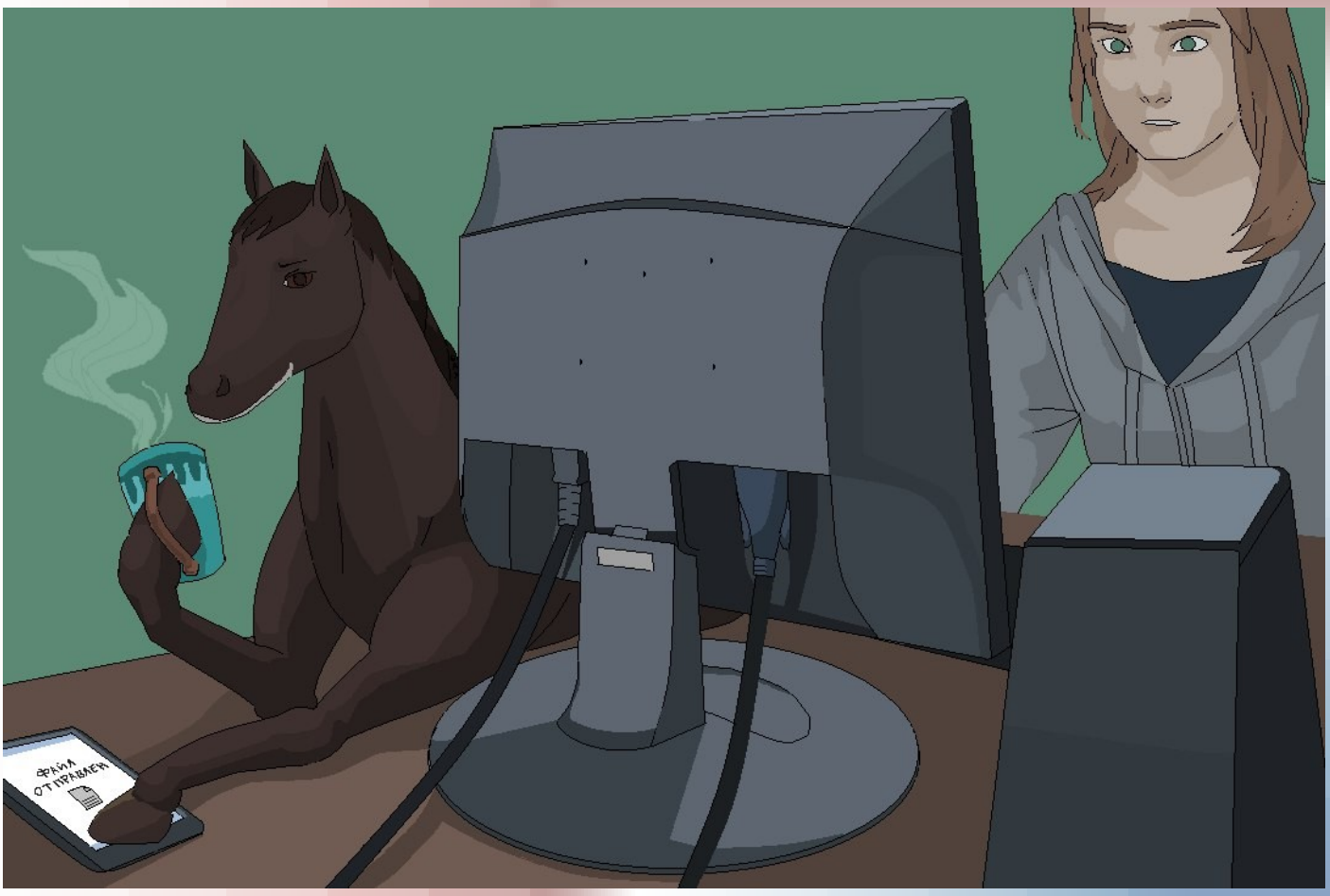
такие «антивирусники» довольно сложно, поскольку программы такого типа, сами защищают себя от удаления. Чтобы обезопасить себя от такого вида мошенничества нужно выполнять несколько

несложных правил: вместо того, чтобы хранить пароли на жестком диске, лучше записывайте их в тетрадь/блокнот; не качайте файлы с подозрительных сайтов и тем более не переходите по сомнительным ссылкам; никогда никому не говорите свои пароли, не вводите пароли в спамах анкеты, помните, что почтовые сервисы никогда не просят пользователей предоставить им какой-то пароль. Следуя этим правилам, можно максимально снизите вероятность подхватить вирус в Интернете.

Все чаще в новостных лентах мы видим сообщения о различных преступлениях совершенных с помощью Интернета. Интернет-мошенничества становятся все более популярными среди преступников. Итак, мы подходим ко второй угрозе – мошенничество. Давайте же разберемся, как обезопасить себя от мошенников? В современном мире очень популярными становятся интернет-магазины, но и там нас может подстерегать опасность. Покупая товары через интернет, нужно обратить внимание на данные продавца (Ф.И.О., электронная почта и адрес) Если продавец указал минимум информации о себе и оставил только адрес своего электронного ящика, это может быть мошенник. Если рядом с фотографиями товаров на сайте имеются отзывы покупателей, обязательно прочтите их. Теперь рассмотрим электронные платежи. Если вы работаете с электронными платежами, в обязательном порядке проверяйте наличие аттестата у продавца интернет - товаров. Если вы увидели, что аттестат отсутствует, и продавец не имеет даже персонального начального аттестата – задумайтесь, стоит ли ему доверять. Распространенным мошенническим ходом является предложение огромных денег за легкую работу. Такие работодатели не только не заплатят вам ни копейки, но и обманным путем завладеют вашими деньгами. Будьте более внимательными и не сотрудничайте с подозрительными фирмами.

Надеюсь, что статья поможет вам избежать различных опасностей/угроз, которые в Интернете мы можем встретить на каждом шагу. Главное – будьте внимательны, не доверяйте рекламам и ярким любопытным вывескам.

Материал подготовила Ульяна Кольцова, 9Б



Компьютерная графика Светланы Бажановой, 8Б

В этом году Светлана стала лауреатом районного интерактивного конкурса компьютерных рисунков и роликов «Безопасный Интернет »

Дети об Интернете

Интернет—это величайшее творение человечества, но что таит в себе эта мировая паутина? Мы попросили ребят из 6Б класса назвать плюсы и минусы интернета и были удивлены тем, как много они об этом знают.

ПЛЮСЫ

- На любые вопросы можно найти ответы
- Помогает делать работы для школы и института
- Позволяет общаться на расстоянии
- Расширяет кругозор
- Помогает определить местоположение и добраться до нужной точки
- Там можно совершать покупки
- Позволяет читать книги, играть, общаться
- Большое количество полезных источников
- Обучение без учителей
- Много фильмов, музыки
- Есть обучающие видеоуроки
- Можно попросить помощи
- Виртуальные путешествия

МИНУСЫ

- Встречаются мошенники
- Неприличные рекламы и комментарии, мат
- Лживые сайты
- Интернет зависимость и психические расстройства
- Подмена реальности Интернетом
- Вирусы, угрозы, спам
- Ухудшение осанки, зрения
- Пиратство
- Люди могут повергаться внушению
- Порнографические сайты
- Сайты, призывающие к расизму, экстремизму, суициду
- Вредит активному образу жизни
- Убивает время

Ребята, помните, что работу за компьютером, чтобы она не стала губительной для здоровья, следует чередовать с активным образом жизни: прогулками, спортом, закаливанием. Ходите на занятия по интересам, в музеи, театры. Больше общайтесь со своими друзьями вживую.

Как обеспечить свою защиту?

Компьютер, подключенный к Интернету, подвергается множеству угроз. Жертвами киберпреступников, как правило, становятся не продвинутые программисты и эксперты, а обычные пользователи, которых сегодня в сети подавляющее большинство. Злоумышленники пользуются тем, что рядовой пользователь мало информирован о потенциальных опасностях интернета, и вследствие этого совершает типичные ошибки – месяцами не меняет пароли, оставляет избыточную информацию о себе в открытом доступе, не пользуется защитными программами. Вот пример тех угроз, что могут ожидать каждого из нас при работе в сети Интернет.

Вирусы - компьютерные вирусы, сетевые и почтовые черви могут распространяться самостоятельно. Например, если вам приходит подозрительное электронное письмо с вложением – весьма высока вероятность того, что оно содержит компьютерный вирус, который может заразить некоторые файлы на вашем компьютере, испортить или украсть какие-нибудь данные. Троянские программы самостоятельно не распространяются, хотя они могут распространяться с помощью компьютерных вирусов. Их основные цели – красть и уничтожать.

неосторожность пользователя – это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере. Например, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления важных данных.

Как обеспечить свою защиту:

1) Устанавливайте на компьютер провереннве антивирусы.

2) Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы и не переходите по содержащимся в них подозрительным ссылкам.

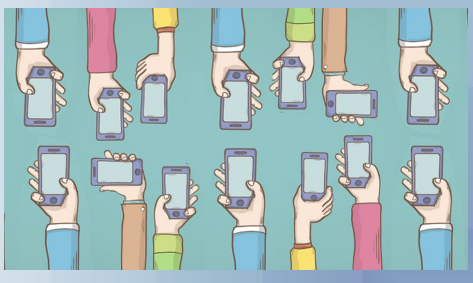
3) Не используйте простые пароли. Нельзя в качестве паролей использовать простые комбинации символов, вроде "qwerty" или "666666". Такой пароль будет взломан программой для перебора паролей за считанные секунды. Не используйте короткие пароли (меньше 6 символов), не используйте в качестве паролей слова, которые есть в словаре. Не используйте один и тот же пароль на все случаи жизни.

4) Будьте осторожны при выходе в интернет из мест общего пользования (например, интернет-кафе), а также при использовании прокси-серверов. Пароли, который вы вводите, в этом случае, с большей вероятностью могут быть украдены.

5) При использовании электронных платёжных систем типа webmoney или яндекс-деньги, работа с ними через веб-интерфейс является менее безопасной, чем если вы скачаете и установите специальную программу (webmoney keeper или интернет-кошелёк для яндекса).

6) Не посещайте сайты с сомнительным содержанием.

7) Даже если у вас безлимитный доступ, всё равно следите за траффиком - его непонятное возрастание может быть свидетельством активности вредоносной программы, а также отключайте соединение с интернетом тогда, когда оно не используется.



Материал подготовила Алёна Тигина, 9Б

Рисунок Светланы Бажановой,

В ВЫПУСКЕ ПРИНИМАЛИ УЧАСТИЕ :

Редакция газеты: Светлана Бажанова - 8Б, Анастасия Подгорная - 9А, Алёна Тигина - 9Б, Ульяна Кольцова - 9Б.
Спасибо за помощь в выпуске учащимся 6Б и 9-х классов.
Вёрстка: Алёна Тигина –9Б.
Ответственная за выпуск: С.А.Смирнова.
Адрес школы: г. Нижний Новгород, ул. Автомеханическая, 13А.

RSPR 52-02166-Г-01
Зарегистрировано в Реестре школьной прессы России. Portal.lgo.ru