Безопасная работа в социальных сетях: общение, публикация материалов.

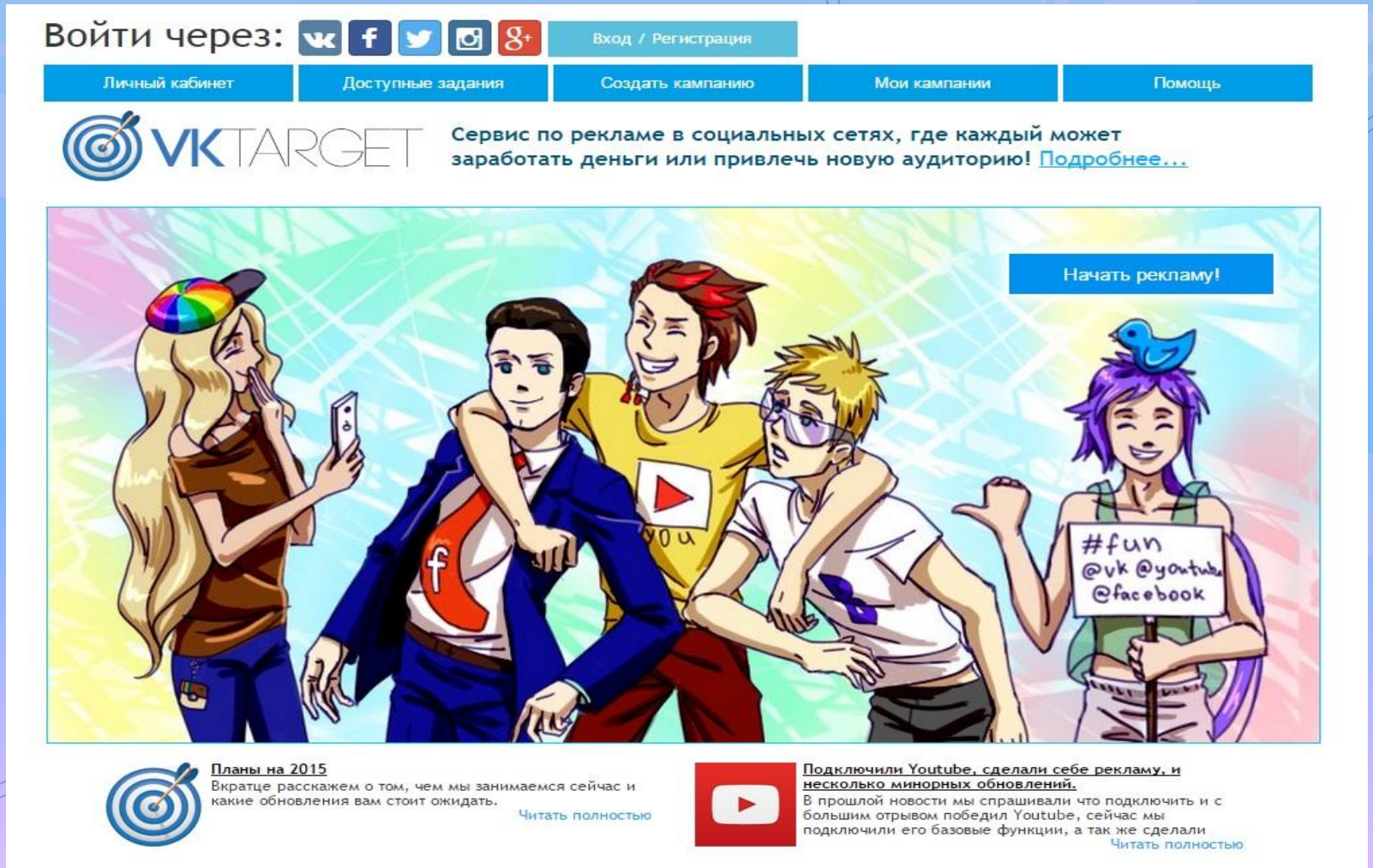
РАБОТУ ВЫПОЛНИЛА УЧЕНИЦА 8" Б" КЛАССА
СРЕДНЕЙ ШКОЛЫ №54 Г. КИРОВА
ЛЫСОВА АНГЕЛИНА

"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

Социальная сеть

Социальная сеть - это онлайн - сервис, предназначенный для общения людей между собой, распространению информации, строенью взаимоотношения в Интернете.

В наше время в интернете существует множество социальных сетей ,такие как Facebook, Google+, Одноклассники, В Контакте, Twitter, YouTube, Instagram и другие. Сейчас они очень популярны. Это привлекает мошенников.



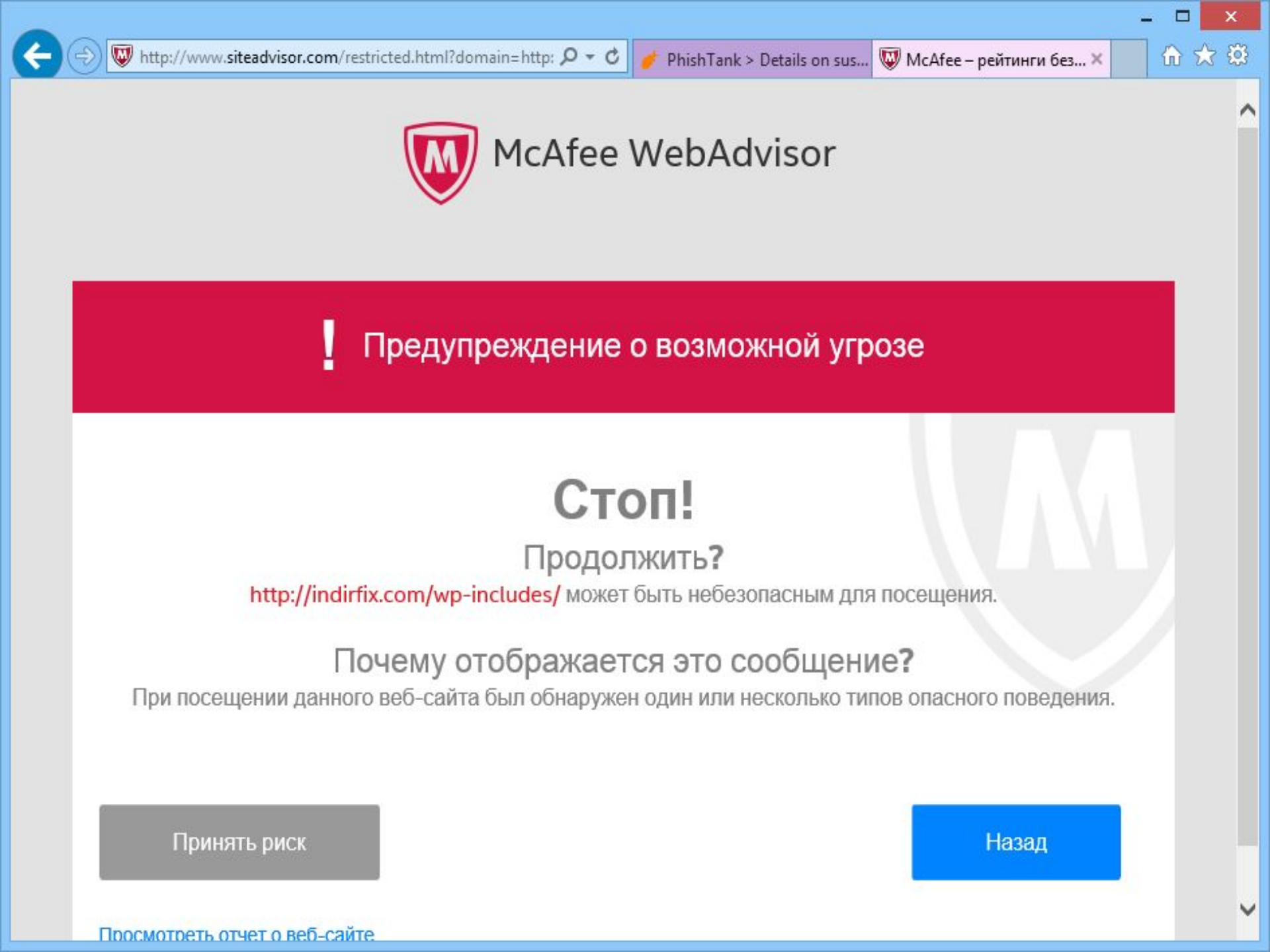
Правила безопасной работы в социальных сетях

Что бы обезопасить себя нужно соблюдать правила безопасной работы в социальных сетях. Нужно знать и выполнять самые простые меры безопасности.

1. **Подходить ответственно к выбору социальной сети.**
   - Регистрироваться только в проверенных социальных сетях, которые могут обеспечить безопасность ваших персональных данных.
   - Перед регистрацией ознакомиться с правилами социальной сети.
   - Регистрироваться только в том случае, если правила сети устраивают.

2.Необходимо следить за адресами, на которые ведут ссылки.

- С начало нужно узнать адрес, на который ведет ссылка. Необходимо навести на нее курсор.
- Не переходить по незнакомым ссылкам, которые приходят вам на почту или в социальные сети.
- Перед тем, как зарегистрироваться проверьте адресную строку браузера.
- Современные поисковые системы и браузеры умеют предупреждать пользователя, когда он пытается зайти на сайт распространяющий вирусы.
- Внимательно относитесь к таким предупреждениям.


http://www.siteadvisor.com/restricted.html?domain=http:
PhishTank > Details on sus...
McAfee – рейтинги без...
McAfee WebAdvisor
Предупреждение о возможной угрозе
Стоп!
Продолжить?
http://indirfix.com/wp-includes/ может быть небезопасным для посещения.
Почему отображается это сообщение?
При посещении данного веб-сайта был обнаружен один или несколько типов опасного поведения.
Принять риск
Назад
Просмотреть отчет о веб-сайте

3.Нужно использовать сложный пароль при регистрации.

- Пароль должен содержать в себе буквы, цифры и специальные символы.
- Чем длиннее пароль, тем сложнее его взломать злоумышленнику.

4.Никому не сообщать пароль к своей странице в социальной сети.

- С осторожностью относитесь к электронным письмам, которые присланы от имени администратора.
- Администрация сети никогда не попросит вас сообщить пароль.

5.С осторожностью устанавливать приложения.

- ✔ Это могут быть приложения социальной сети, например, игры для браузеров и программы-клиенты, например, на мобильных устройствах.
- ✔ Эти приложения могут быть использованы для кражи ваших данных в социальной сети.

6.Осмотрительно подходить к выбору друзей.

- Не добавляйте в список друзей всех подряд.
- Среди ваших друзей может оказаться мошенник.
- Пользуясь вашим доверием, он может взломать вашу учетную запись.

7.При завершении работы в социальной сети обязательно выполнять процедуру выхода.

- Всегда выполняйте процедуру выхода, потому что к вашим персональным данным могут получить доступ другие люди.

8.Данные о себе, которые вы размещали в социальной сети, могут попасть в руки злоумышленников.

- Даже после удаления учетной записи, кто-то может сохранить все данные, которые были на ней.

9.При подозрении на взлом учетной записи.

- Если вы подозреваете, что кто-то узнал ваш пароль к учетной записи, то сметите его немедленно.
- Это повысить уровень безопасности.

10.Не нажимайте на подозрительную рекламу в интернете.

Наличие антивирусной программы полностью не защитит ваш компьютер. Его безопасность зависит только от вас. Если вы будете выполнять эти простые правила, то ваш компьютер будет в полном порядке. И вам не придётся тратить деньги, и время на его починку.

Следите за своей безопасной работой в социальных сетях!!!

Спасибо за