

БЕЗОПАСНАЯ РАБОТА В СОЦИАЛЬНЫХ СЕТЯХ: ОБЩЕНИЕ, ПУБЛИКАЦИЯ МАТЕРИАЛОВ.

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

Выполнила: Соколова Регина М. ,
учащимся 11 класса , МАОУ
гимназии №115, Советского района





БЕЗОПАСНАЯ РАБОТА В ИНТЕРНЕТЕ: 10 ПРАВИЛ



- **1**- Необходимо следить за адресами, на которые ведут ссылки. Для того чтобы узнать адрес, на который ведет ссылка необходимо просто навести на нее курсор. Если вам предлагают перейти на сайт X, а ссылка ведет на сайт Y то тут что-то не так. Возможно, вас попытаются обмануть.



- ⦿ **2.** Перед вводом личной информации проверяйте адресную строку браузера. Если вы там увидите что то вроде vkontokte.ru вместо привычного vkontakte.ru, то можете быть уверены, что вы находитесь на поддельном сайте и у вас пытаются украсть пароль для доступа к вашему аккаунту. После получения данных злоумышленники могут использовать аккаунт для рассылки спама и вирусов вашим друзьям.
- ⦿ **3.** Не переходите по незнакомым ссылкам, которые приходят вам на почту, в «аську», или в социальные сети. Даже если ссылка пришла от знакомого человека необходимо быть максимально внимательным. Вполне возможно аккаунт вашего знакомого уже взломан, и теперь от его имени рассылают вирусы.
- ⦿ **4.** Не скачивайте неизвестные файлы, пришедшие вам на почту или в «аську», даже если файл пришел от вашего знакомого. Перед тем как скачивать такие файлы уточните у отправителя, что это за файл.

- **5.** Современные поисковые системы и браузеры умеют предупреждать пользователя, когда он пытается зайти на сайт распространяющий вирусы. Необходимо внимательно относиться к таким предупреждениям, скорее всего сайт, который вы пытаетесь посетить, заражен.
- **6.** Не кликайте по подозрительным рекламным баннерам, предлагающим мгновенное обогащение или другие нереально выгодные услуги и сервисы. Скорее всего, вас пытаются обмануть.
- **7.** Относитесь с подозрением к программам для «взлома» онлайн сервисов, игр и программ. В результате использования таких программ жертвой «взлома» можете стать именно вы.
- **8.** Будьте внимательны к файлам загружаемых через BitTorrent, DirectConnect и другие файлообменные сети. Пользователи данных сетей могут распространять вирусы, даже не подозревая об этом.
- **9.** Не используйте Internet Explorer, особенно его старые версии. Существует большое количество других, более быстрых и безопасных браузеров.
- **10.** Отключите Java Script. Большая часть сайтов отлично работают без использования Java Script. Для браузера Mozilla Firefox можно использовать плагин Noscript, данное расширение позволяет отключать выполнение скриптов только для неизвестных сайтов.

МНОГООБРАЗИЕ СОЦИАЛЬНЫХ СЕТЕЙ:

○ Общение:

- **блоговые сервисы** (Blogger, LiveJournal, Open Diary, и др.);
- **микроблоги** (Twitter, Yammer, Qaiku и др.);
- **соц. сети** (Facebook, V Kontakte, Одноклассники, LinkedIn, Ning, Orkut и др.)
- **сети событий** (Eventful, Upcoming и Meetup).

⊙ **Мультимедиа:**

- **социальные видеохостинги** (YouTube, Vimeo и Zideo);
- **сервисы обмена фото** (Instagram, deviantArt, Picasa и Zoomr);
- **сервисы обмена музыкой** (MySpace Music, Last.fm, ShareTheMusic и ccMixter);
- **Интернет-службы вещания в прямом эфире** (Justin.tv, Skype, Ustream.tv, OpenCU);
- **виртуальные службы обмена презентациями** (Scribd и Slideshare)

⊙ **Сотрудничество:**

- **справочники** (Wikipedia, Wetpaint и PBworks);
 - **социальные закладки** (Delicious, Google Reader, News2.ru, Bobrdobr.ru и др.);
 - **новостные службы** (Digg, NowPublic, Reddit и Mixx).
- Обзоры и авторские точки зрения:**
- **сервисы потребительских обзоров товаров и услуг** (MouthShut.com, Epinions.com и др.);
 - **службы по бизнес-деятельности** (Yelp.com и Customer Lobby);
 - **социальные порталы популярных вопросов и ответов** (WikiAnswers, Yahoo!Answers, Google Answers, Askville и др.).



- ◎ Развлечения:
 - развлекательные платформы (Cisco Eos);
 - онлайн-игры (Аллоды, Троецарствие, World of Warcraft, The Sims Online и др.);
 - сервисы обмена играми (Kongregate и Miniclip).





◎ Спасибо за внимание!

