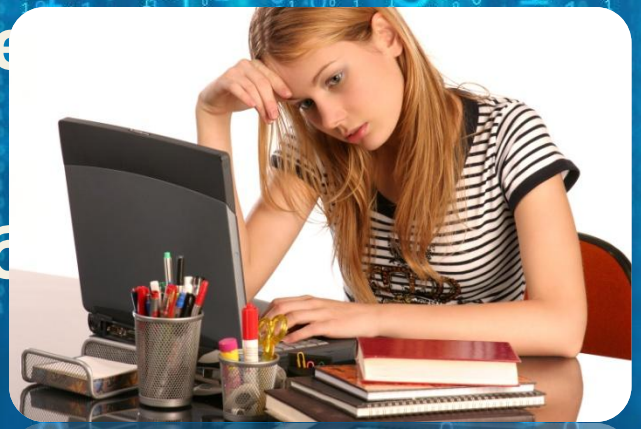
Безопасная работа в социальных сетях: общение, публикация материалов

Вступление

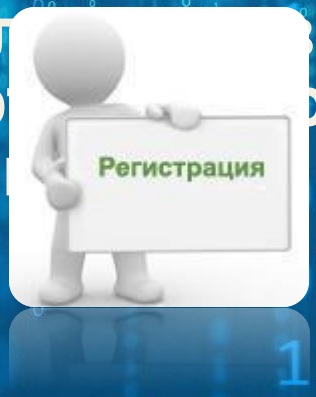
Многие из нас прочно связаны сетями интернета, такими, как: Одноклассники, ВКонтакте, Facebook, Twitter, MySpace. Почти все пользователи социальных сетей забывают о безопасности в них. Мы хотим рассказать вам об основных правилах безопасности в интернете, которые благополучно помогут вам защитить себя и свой компьютер.



Шаг первый: Регистрация

Не стоит регистрироваться без разбора во всех социальных сетях. Лучше зарегистрироваться на одном сайте, который вы будете часто использовать, предварительно изучив политику конфиденциальности. К сайтам, где вы оставляете свои данные, стоит относиться со всей серьезностью.

Обязательно учитывайте вероятность того, что все данные, которые вы выкладываете, могут быть кем-то сохранены. Вы можете удал вою учетную запись, а задолго до э огие люди могут сохранить ваши дан



Шаг второй: Контроль данных

Необходимо контролировать всю информацию о собственных данных, которую вы размещаете в сетях. Злоумышленники обычно осуществляют взлом учетной записи таким образом: используют ссылку «Забыли пароль», которая есть для входа в учетную запись. Для восстановления пароля система зачастую предлагает ответить на секретный вопрос. Это может быть девичья фамилия материи, ваш родной город и т.д. А ответы на эти вопросы можно получить на вашей личной странице в соцсети: эти сведения многие размещают с легкостью. Поэтому не стоит выкладывать особо л мацию и при указании ответа на секрет нужно придумать что-то оригинальное.

Шаг третий: Доверие

Не нужно добавлять в друзья всех подряд. Ведь мошенники часто создают «левые» аккаунты, чтобы заполучить информацию, которая может быть доступна только друзьям.

Не стоит думать, что сообщение, которое получено вами, именно от того человека, от которого указано. Сейчас многие хакеры взламывают учетные записи и распространяют сообщения таким образом, что это выглядит так, как будто сообщение пришло от вашего знакомого или друга. Если у вас появляются подозрения на этот счет, то лучше связаться по телефону со своим знакомым и узнать у него, присылал ли он вам сообщение. Не нужно принимать все приглашения о регистрации в той или иной соцсети.

Нужно с осторожностью переходи пкам, которые приходят к вам от других пользов ужно открывать все ссылки подряд. Нужно сн ться, что полученная ссылка действительно вед асный ресурс.

Шаг четвертый:
Не забывайте о детях!

И, наконец, постарайтесь оградить своих детей от общения в социальных сетях. Как правило, опытные мошенники являются хорошими психологами. Ребенок может выдать информацию о вас и вашей семье без какого-либо злого умысла. Да и педофилов и прочих извращенцев в Интернете развелось не меряно. Если у вашего ребенка все-таки есть своя страница, постоянно контролируйте его переписку и проверяйте друзей. Не давайте преступникам шанс воспользоваться вашей неосмотрительностью и неосторожностью!

Используйте эти п…
социальных сетях будет д…

Спасибо за внимание!

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