Написав Олександр Буржунецький
Середа, 14 липня 2010, 19:19 - Останнє оновлення Четвер, 15 липня 2010, 22:49

Ура! Вы счастливый пользователь "Одноклассников". Десятки, а то и сотни друзей, тысячи групп, поток информации просто ошеломляющий. Но не радуйтесь преждевременно, ибо чем больше и качественнее по содержимому ваша страничка, тем легче потенциальному злоумышленнику получить доступ к вашему аккаунту. Так-что давайте пройдемся по пунктам и уясним для себя, так ли важна или нужна другим та информация, которую Вы собираетесь о себе сообщить или уже сообщили, и на крайний случай для какого круга людей она доступна. Тему социальной инженерии обсуждать здесь бесполезно, на просторах социальных сетей это работает безукоризненно, однако в рамках статьи рассмотрим несколько примеров для наглядности.

Начнем по порядку. Вы регистрируетесь в "Одноклассниках". Если Вы заметили, в поле "логин" допустимы латинские символы а также цифры и некоторые спецсимволы. Возпользуйтесь данной возможностью и придумайте себе логин потяжелее. Чем длиннее логин и чем разнообразнее символы в нем использующиеся, тем труднее и дольше злоумышленнику будет его подобрать или узнать. Никогда не пользуйтесь логином, который состоит из транслитерации, перевода, сокращения, или иного простого изменения каких-либо Ваших данных, которые Вы собираетесь сделать публичными. На крайний случай, если уже совсем ничего не получается используйте какую-либо трансформацию из ваших даных, которые знаете только Вы и никто больше.

Создание пароля.

К вопросу создания пароля отнеситесь серьезно, все вышесказаное о логине относится также и к паролю. Изпользуйте побольше разных символов, цифр знаков, ведь Вы совсем не ходите, что-бы Ваша страница превратилась в проходной двор и каждый желающий мог сделать на ней что угодно. Кстати, если Вы пользуетесь "Одноклассниками" постоянно на одном компьютере, то рекомендую Вам использовать какой-либо из менеджеров паролей - и пароль не забудете, и введут его для Вас автоматически, а заодно и сгенерируют стойкий к взлому. Ни в коем случае не следует полагаться на менеджер паролей в Интернет-браузере - так как эти данные защищены слабо и в результате вирусной деятельности могут быть скомпроментированы.

E-мейл.

Конечно же, идеальным вариантом было бы использование отдельного почтового ящика для данного сервиса. Если у Вас есть возможность, попросите провайдера открыть Вам дополнительный почтовый ящик, сейчас провайдеры поголовно инеют такую услугу. Если же нет, откройте ящик на каком-либо бесплатном сервисе: Google, Yahoo, Яндекс и т.д. Однако к выбору сервиса для открытия почтового ящика нужно подходить осторожно, сейчас на просторах интернета тысячи такого рода сервисов, и немалая часть из них кишит дырами не меньше чем голландский сыр. Ну и наконец можно вообще обойтись без почтового ящика, а придумать контрольный вопрос на который знаеете ответ только Вы. Меня иногда поражает скудность выбора контрольных вопросов разных сервисов и если возможно, то выбирайте пункт сформулировать вопрос самим и соответственно запишите ответ. Помните, что несмотря на кажущуюся сложность сформулированного вопроса, подчас даже незнающий Вас человек, сможет подобрать ответ за 2-3 минуты. Это я к вопросам типа "мой размер лифчика/сапог/кросовок и т.д.". Извините если загнал кого-нибудь в "краску".

Регламент и соглашение пользователя.

Старайтесь как ни банально это бы звучало все-таки ознакомится с регламентом работы сервиса, с пользовательским соглашением. Полезную информацию о безопасности можно почерпнуть и там. Вконце концов этими правилами регламентируется Ваше поведение в "Однокласниках" и Вы согласились их выполнять.

Тепер Вы "почти" обезопасили свой аккаунт от посягательства сторонних пользователей. Почему почти? Потому что вопрос о безопасности на этом не исчерпывается. И речь далее пойдет не только о несанкционированном доступе к вашему аккаунту в социальной сети, а даже о Вашей лично безопасности, а также безопасности Вашей семьи. Но сначала рассмотрим самую, наверно, распространенную ошибку в поведении в сети - невнимательность. Итак, Вы на своей странице. Добавьте свою страницу в закладки и в дальнейшем заходите в свой аккаунт через сделанную закладку. Довольно ефективная мера от подмены страницы для логина/пароля и опечаток при вводе адреса, а также следования по присланным линкам якобы на сайт. Никогда не спешите, акуратно прочитайте письмо, сообщение или приглашение перед тем как ввести туда свои данные. Возможно это сайт-двойник, собирающий ваши учетные данные которые Вы сами же ему по невнимательности и сообщите. Лучше, если Вы получили письмо с портала, зайти в браузер и открыть запомненную закладку чем сдать свои логин и пароль на первом попавшемся сайте-мошеннике. Читайте письма внимательно, подчас подложные письма выглядят точь в точь как настоящие. Внимательно смотрите на линк по которому собираетесь перейти, если Вы собираетесь

кликнуть на ссылку прочитать/войти или какую другую, а при наведении мыши на ссылку в нижней строке значится что-то вроде jygsaytad.com, то лучше воздержаться и удалить даное послание. Ведь в любом случае, входя на "Однокласники" сервис Вам покажет новое письмо или изменения которые произошли за время Вашего отсутствия.

Возможно, Вы уже получили письмо "счастья" от кого-либо из друзей, причем стиль изложения явно не соответствует поведению Вашего друга, или такого рода сообщения ему не свойственны. Старайтесь выяснить этот вопрос с помощью других каналов связи, так как, скорее всего, его учетная запись уже взломана. Не стоит писать гневных писем, ведь он, тоесть друг, даже и не ведает, что он уже "успел" в "Одноклассниках" разослать тысячу писем с приглашением посетить порно-ресурс или зарегистрироваться в на каком-либо другом сайте.

Для начала на этом остановимся. В следующей части рассмотрим информацию которую Вы публикуете или собираетесь опубликовать на своей странице.