УДК: 004.056.52

Защита аккаунтов в социальных сетях

Жданов А.А. Группа 11-ИБ

В современном мире все большее значение имеет информационная безопасность каждого человека. Сегодня особой популярностью пользуются социальные сети. Люди привыкли общаться в сети, обмениваться личной информацией и фотоснимками. Но многие аккаунты в соцсетях защищены не надежно защищен. Поэтому, некоторые меры безопасности для защиты от взлома странички не помешают. Рассмотрим основные из них.

Пароль — это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация «имя пользователя — пароль» используется для удостоверения пользователя.

Как правило, взламывают с целью использования вас для отправки спама, или же для массовой продажи взломанных профилей тем кто занимается рассылкой этого спама. Взломы с этой целью носят массовый характер, тоесть взломать всех подряд не выбирая.

Прямой перебор. Перебор всех возможных сочетаний допустимых в пароле символов.

Подбор по словарю. Метод основан на предположении, что в пароле используются существующие слова какого-либо языка либо их сочетания.

Метод социальной инженерии. Основан на предположении, что пользователь использовал в качестве пароля личные сведения, такие как его имя или фамилия, дата рождения и т.п.

Пароль типа «123456» или «qwerty». Такой пароль легко запоминается, но подбирается ручным подбором примерно за 5 минут. Кстати, такие пароли используют примерно 5% всех пользователей Интернета. Специальная

программа «вычисляет» такой пароль в течении примерно микросекунды.

Пароль, состоящий из осмысленного (разговорного) английского слова длинной до 10 букв подбирается специальной программой в среднем за 2 секунды**.**

Пароль из четырех английских символов, включая цифры и спецсимволы (типа hd4$) «противостоит взлому» уже примерно 3 минуты, а такой же пароль из букв разного регистра, цифр и хотя бы одного спецсимвола из семи знаков «держится» уже примерно 30 суток.

И никогда не использовать в качестве пароля своё имя, фамилию или дату рождения. Такой пароль легко подберет любой человек, который Вас знает.

Не передавать свой логин и пароль. Если есть подозрение – менять пароль. Полезно и просто регулярно менять пароль, базы паролей регулярно «вскрываются » и продаются на «черном» Интернет-рынке.

Необходимо применять для разных аккаунтов разные логины и пароли. Даже если злоумышленник «вскроет» один из Ваших акаунтов, к другому та же пара «логин+пароль» просто не подойдет.

Антивирус не просто должен быть, он должен регулярно обновляться! Новые «трояны» - программы шпионы, пересылающие данные с Вашего компьютера совершенствуются с ужасающей быстротой!

Лучше не держать пароли в отдельном файле на компьютере, а скинуть ихна защищённый паролем носитель или записать на бумагу. Только вот, «бумажка » эта не должна попасть в чужие руки.

Почтовые ящики на бесплатных почтовых серверах «вскрываются» особенно часто. Так, что, получив на такой ящик данные («логин+пароль»), сразу копируйте их на компьютер и удаляйте с ящика.

Обязательно установите на свой компьютер надежную антивирусную программу. Лидерами в защите от вредоносных программ являются антивирусы «Касперского», Nod32 и Dr.Web. Если на ПК присутствует антивирусная программа, то файлы cookies, в которых и хранится персональная информация о логинах и паролях, не смогут легко попасть в руки «недруга».

Важным моментом в защите аккаунта является наличие программы-барьера, или firewall, на компьютере. В настойках этого приложения можно указать правила поведения при соединении с почтой, сайтом соц. сети или ICQ. «Фаервол» способен выявлять трояны и черви, которые передают персональные данные пользователя другому юзеру в сети. Данная программа просто не заменима для тех людей, которые занимаются финансовой деятельностью в интернете. Помните, что такие приложения часто встроенные в антивирусную программу.

При комплексной защите аккаунта в социальной сети следует внимательно относиться к скачиваемой информации. Не стоит уделять внимание бесплатным программам сомнительного содержания. Следует игнорировать загрузку разных кряков и кейгенов, поскольку они способны занести на ПК вредоносную программу или код. Проверка на вирусы перед закачкой подобных файлов обязательна!

Особое внимание нужно обращать на ссылки, которые приходят в приватных сообщениях от друзей. Этот линк мог оставить хакер, предварительно взломав аккаунт этого адресанта. Обычно ссылка рекламирует какой-либо продукт или предлагает просмотреть интересные фотографии. Перейдя по ней, происходит перенаправление и, не исключено, что персональные данные попадают в руки «злоумышленника».

Приведенные выше рекомендации помогут защитить аккаунт и обеспечат нервную работу хакеру, который собирается завладеть чужими персональными данными.

Список литературы:

1.Захист - Аналитика [Электронный ресурс]: (с изменениями и дополнениями) - Режим доступа: http://www.zahist.narod.ru/passw_crack12.htm (дата обращения 17.10.2012)

2.Материал из Википедии [Электронный ресурс]: (с изменениями и

дополнениями) - Режим доступа: http://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C (дата обращения 17.10.2012)

3.Защита аккаунтов в социальных сетях [Электронный ресурс]: (с изменениями и дополнениями) - Режим доступа: http://smilebar.ru/zaschita-akaunta-v-socialnoi-seti (дата обращения 17.10.2012)