РИСКИ В СОЦИАЛЬНОЙ СЕТИ

- Самый главный риск – это потеря персональных данных и информации для доступа к аккаунту. Потеря контроля за профайлом (краткие сведения о пользователе: дата рождения, имя, ник, когда зарегистрирован, увлечения и прочая информация) может привести к различным последствиям, таким как рассылка спама и зараженных файлов от твоего имени или опубликование твоей переписки с друзьями;
- Информация, которая появляется в интернете в отношении тебя, может очень повлиять на тебя сейчас и в будущем. Например, ты можешь показывать, что ты лентяй или можешь быть очень вульгарным в общении в социальной сети, что характеризует тебя с плохой стороны. Именно такой вывод сделает менеджер по персоналу, который будет принимать решение о приеме тебя на работу.
- Ты можешь заинтересовать не только кибер, но и других преступников. Например, размещая информацию о своей квартире, благосостоянии твоей семьи, сообщая куда ты с семьей поедешь на каникулы, ты можешь заинтересовать воров;
- Ты можешь спровоцировать травлю себя со стороны пользователей сети;
- Также через социальные сети возможно заражение твоего компьютера.

Стоит отдельно рассказать про взлом профайла, и о том, как злоумышленники получают доступ к аккаунту. Вот некоторые самые популярные методы получения пароля:

- посредством перебора пароля по словарю или ручного подбора самых часто используемых простых паролей;
- Путем прямого контакта с жертвой и выяснения, что может быть паролем. Метод очень опасен для тебя, если применяется опытным человеком. Не надо никому сообщать свои личные данные, даже если этот человек будет представляться сотрудником техподдержки или администрации;
- В интернет-кафе, а также у друзей, которые хотели бы получить твой пароль. Киберпреступники могут использовать программы, называемые KeyLogger-ами – это клавиатурные шпионы, перехватывающие нажатия на клавиатуру и записывающие их в файл, таким образом, злоумышленник сможет получить твой пароль. Такая программа может быть установлена на любом общественном компьютере, в том числе в интернет-кафе;
- Получить доступ к твоему профайлу можно через отсылку письма с просьбой перейти по ссылке и там ввести свои данные, или просто выслать свои данные для перерегистрации, представляясь сотрудниками портала. Вариантов много, а цель одна – через письмо человек вводит свой пароль, а злоумышленники его получают. В этом случае ты практически безвозвратно теряешь свою почту и все свои аккаунты, зарегистрированные на нее;
- Программные методы. Этот метод взлома доступен знающим людям и состоит в поиске ошибок в коде сайтов, позволяющих получить доступ к базе данных с паролями. В таком случае данные могут восстановить только администраторы;
- Метод обмана – очень распространенный метод доступа к личным данным. Сюда входят предложения
  - скачать всевозможные программы, на самом деле являющиеся опасными вирусами, которые не всегда сразу определяются антивирусами
  - загрузить фото вместо граффити, установить новые смайлики
  - отправить cookies, логин и пароль в адрес неких людей, которые представляются сотрудниками техподдержки или администрации.
- Взлом твоего компьютера, где киберпреступники находят пароли. Это очень сложный способ и очень часто антивирусные программы замечают подобную деятельность. Обычно используются троянские программы.

Педагог-психолог: Наговицина Е.О.

Информация с сайта сетевичок.рф