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;
- 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.
- 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.
- Программные методы взлома доступны 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.

ГБУ РЦПМСС «Сайзырал» 667001,
Республика Тыва,
г. Кызыл,
ул. Рабочая,56 тел., факс 5-33-20
e-mail: rzpmss@yandex.ru

Подготовила Шактар-оол Б.В.,
педагог-психолог

Государственное бюджетное учреждение
Республиканский Центр психолого-медико-социального сопровождения

Социальные сети

Кызыл-2019

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек. Социальные сети, начались в 1995 году с американского портала Classmates.com

В Россию мода на социальные сети пришла в 2006 г., с появлением Одноклассников и ВКонтакте.

Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. Известен случай проявления психологического расстройства на почве зависимости от общения в социальных сетях.

Риски в социальной сети

- 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 рассылке 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.
- 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.

Основные советы по безопасности аккаунта в онлайн-играх:

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.
- Будь в курсе классификаций и возрастных ограничений в игре.
- Не указывай личную информацию в профайле игры. Таким образом, другие игроки не смогут тебя найти, и ты будешь в безопасности.
- Уважай других участников по игре.
- Не устанавливай неофициальные патчи и моды.
- Используй сложные и разные пароли.
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.
- Остерегайся игр в социальных сетях. Когда ты даешь доступ к твоему профилю, ты даешь злоумышленникам шанс получить твои личные данные.