СОЦИАЛЬНЫЕ СЕТИ

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты.

«Новый тренд» в Интернете, социальные сети, начались в 1995 году с американского портала Classmates.com («Одноклассники» являются его русским аналогом). Проект оказался весьма успешным, что в следующие несколько лет спровоцировало появление десятка похожих сервисов. Но официальным началом бума социальных сетей принято считать 2003—2004 годы, когда были запущены LinkedIn, MySpace и Facebook. В Россию мода на социальные сети пришла двумя годами позже — в 2006-м, с появлением Одноклассников и ВКонтакте.

И если LinkedIn создавалась с целью установления деловых контактов, то владельцы MySpace и Facebook сделали ставку в первую очередь на удовлетворение человеческой потребности в самовыражении. Социальные сети стали своего рода Интернет-пристанищем, где каждый может найти базу для создания своего виртуального «Я». При этом каждый пользователь получил возможность не просто общаться и творить, но и делиться плодами своего творчества с многомиллионной аудиторией той или иной социальной сети.

Однако 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. Информацию об участниках социальных сетей могут найти их работодатели, бывшие или настоящие жены или мужья, сборщики долгов, преступники, правоохранительные органы и так далее.

Известен случай проявления психологического расстройства на почве зависимости от общения в социальных сетях. В Белграде девушка Снежана Павлович попала в психиатрическую клинику после того, как её заметка в социальной сети Facebook не вызвала интереса среди её друзей. Врачи клиники назвали этот случай «синдром Снежаны», объясняя поведение пациентки как обычный стресс от неудовлетворенности социальной потребности индивидуума в современном мире.

КАКИЕ РИСКИ СУЩЕСТВУЮТ 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.

ОСНОВНЫЕ СОВЕТЫ ПО БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.

- Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- Используй настройки конфиденциальности аккаунта. Настрой просмотр содержимого твоей учетной записи "только для друзей". Таким образом, незнакомые люди не увидят твою личную информацию;
- Принимай запросы в друзья только от тех людей, которых ты знаешь и которым доверяешь;
- Не используй веб-камеру для общения с людьми, которых ты не знаешь;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Будь осторожен - некоторые пользователи могут представляться кем угодно;
- Если ты действительно хочешь встретиться с человеком, с которым познакомился в интернете, то договорись о встрече в общественном месте и желательно взять с собой кого-то еще, например, друга. Если твой сетевой друг считает, что присутствие кого-то еще плохая идея, то стоит отказаться от встречи;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу;
- Не размещай фотографии и видео со своими друзьями без их разрешения. Обращайся к друзьям, чтобы они также соблюдали конфиденциальность и не размещали твои фотографии и видео в общем доступе;
- Никогда не открывай подозрительные ссылки, даже если они пришли от твоих друзей. Удостоверься в том, что друг тебе выслал эту ссылку сам, а его аккаунт не контролирует киберпреступник. После взлома аккаунта злоумышленники в первую очередь делают рассылку по адресной книге, а поскольку доверие друзей друг другу выше, то вероятность заражения вирусами резко вырастает;
- Чтобы попасть в свою социальную сеть или на какой-либо другой сайт лучше используй закладки или окно быстрого доступа. Таким образом, ты точно попадешь на те порталы, которые безопасны и которыми ты пользуешься. При наборе адреса есть риск того, что ты ошибешься с адресом и не заметишь этого.