

Как обезопасить свой профиль в социальных сетях?

ВКонтакте, Фейсбук, Твиттер, Одноклассники — в соцсети мы заходим ежедневно: читаем, смотрим, что случилось у друзей и знакомых, делимся событиями из своей жизни. Сами добровольно отказываемся от анонимности. При этом в реальности мы не готовы пускать в свой дом, в свою жизнь всех подряд, но с легкостью делаем это в цифровой жизни.

Живя в сети, тоже необходимо устанавливать границы, где заканчивается личное пространство и начинается общественное. Спросите себя:

- как вы готовы взаимодействовать с другими и оставаться при этом защищенным?

- где заканчивается неприкосновенность вашей частной жизни?

- какую информацию вы хотите сохранить в тайне?

Восемь советов для защиты своей страницы в соцсети

1. вы не обязаны указывать настоящее имя, если есть желание скрыть его — используйте псевдоним;

2. при регистрации не давайте больше информации, чем это необходимо. Если хотите скрыть себя, заведите отдельную электронную почту, которую будете указывать при регистрации. Но имейте в виду, что ваш IP-адрес может быть внесен в лог сервера соцсети при регистрации. И если вы нарушите закон страны проживания — вас легко можно будет вычислить;

3. выберите надежный пароль и, если возможно, включите двухфакторную аутентификацию (например, когда соцсеть или сайт для подтверждения вашей личности попросит ввести не только пароль, но и код доступа, отправленный на телефонный номер);

4. используйте защищённое соединение (HTTPS) при работе с соцсетями;

5. если вы зашли в соцсеть с чужого компьютера, например, из библиотеки или в кафе, не забудьте потом выйти со своей страницы (а не просто закрыть окно браузера). Очистите историю браузера/кеш. Дома поменяйте пароль;

6. когда для восстановления пароля устанавливаете контрольный вопрос, избегайте тех, ответы на которые можно получить с вашей страницы в соцсети. Например: «В каком городе вы родились?» или «Имя вашего питомца»? Как вариант, вы можете выбрать для восстановления пароля ответы, которые являются ложными. Только не забудьте их сами.

7. никогда не нажимайте на ссылки, присланные незнакомыми пользователями ВКонтакте, Фейсбука, Твиттера и других социальных сетей. Если не уверены, что присланная вам ссылка — настоящая, проверьте ее при помощи специальных сервисов, таких как [VirusTotal](#).

8. не пренебрегайте настройками приватности, которые есть в каждой социальной сети. Только вам решать, кто может добавлять записи на вашу стену; могут ли другие люди отмечать вас в своих постах; кто может видеть ваши посты, фотографии и личные данные; кто может оставлять вам сообщения — все или для этого потребуется добавиться в друзья.