Проблема сохранения персональных данных в Интернете встала особенно остро в связи с увеличением случаев мошенничества, киберпреследования и запугивания пользователей. Выложить в Twitter фотографию своей банковской карты? Легко! Разместить скан паспорта в Инстаграме? Конечно! Опубликовать служебные пароли Вконтакте? Без проблем!

Получив личную информацию о жертве, злоумышленник с легкостью может испортить ей жизнь или даже подорвать материальное благосостояние. Поэтому так важно держать свои персональные данные в секрете, скрываясь под многочисленными никами, номерами и нейтральными учетными записями, чтобы избежать неприятностей. Однако, в связи с желанием многих пользователей пользоваться социальными сетями и сайтами знакомств, скрывать всю информацию о себе не представляется возможным. Как иначе зарегистрироваться на «Одноклассниках», если не указывать имя, фамилию и учебные заведения? Как завести знакомство с девушкой/парнем на сайте, не опубликовав фотографию и способы связи?

Наше пособие поможет пользователям защититься от подобных угроз.

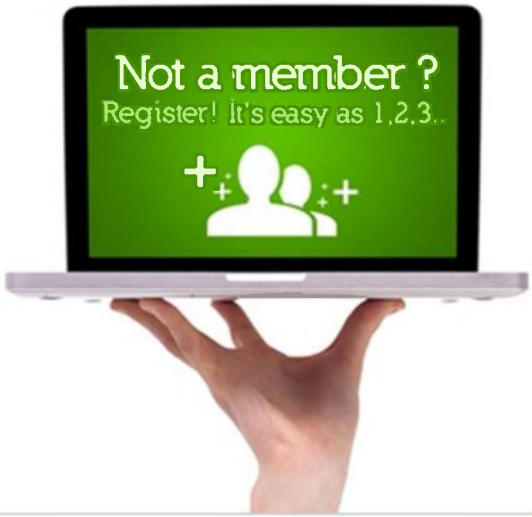
МБУК «Межпоселенческая библиотека Выборгского района»

Центр правовой информации
г. Выборг, ул. Рубежная, 18,
Ул. Пионерская, 4

Телефон: (81378)20059
Эл. почта: bibinternet@yandex.ru
ВКонтакте: http://vk.com/bibpravo

МБУК «Межпоселенческая библиотека Выборгского района»

Как защититься от негативного использования персональной информации в социальных сетях



Безопасный интернет

Советы по защите персональной информации в социальных сетях

1. По возможности используйте псевдонимы.

2. Указывайте лишь электронные способы связи, причем созданные специально для таких контактов.

Например, специально выделенный для подобного общения e-mail. Если собеседник окажется интересным и безопасным, ничто не мешает поделиться с ним потом «более реальными» электронными координатами, а то и телефоном или адресом.

3. Тщательно обдумайте, какую информацию о себе загружать в Интернет.

В Интернете действует принцип «все, что вы выложили, может быть использовано против вас». Даже если вы удалите фото, его уже могли скопировать – а значит, оно по-прежнему ходит по Интернету. Например, фото разгульной вечеринки может вызвать разрыв с близким человеком, видеоролик драки – стать доказательством для суда, демонстрация богатства наведет на вас грабителей, а подробные данные о себе подскажут им, где и как вас лучше ограбить.

4. Осторожно подходите к выбору друзей, не принимайте все заявки подряд для количества.

Радость от большого числа «друзей» быстро омрачится неприятностями. Другом в соцсети может быть только тот, кто хорошо известен – желательно в реальной жизни.

5. Не открывайте доступ к своим личным страничкам незнакомым людям.

Есть те, кто специально ходит по социальным сетям с целью сбора информации. Мошенники, спамеры, фишеры могут воспользоваться вашими фотографиями и контактами для размещения на других ресурсах, где бы вы совсем не хотели их видеть. Получив информацию о вас, они непременно включат ее «в свой оборот», используя ее для киберпреследования или подготовки серьезных преступлений. Чем меньше вы им дадите информации о себе – тем безопаснее.

Доверчиво публиковать информацию о себе, понадеявшись лишь только на то, что вряд ли кто-то увидит ее кроме самых близких людей, - ошибка многих пользователей.

Помните, что большая часть приложений социальных сетей предназначена для доступа к конфиденциальной информации, кроме того, при использовании конфиденциальной информации в противоправных действиях, их доступность и публичность вряд ли поможет вам оправдаться и избежать ответственности.

Всегда старайтесь оставить о себе минимум информации, не сообщайте ничего лишнего, не открывайте доступ к своим личным страничкам незнакомым людям и общение в социальных сетях принесет максимум удовольствия и минимум проблем.