Функция вполне удобная: можно открыть карту и посмотреть, в каких местах вы делали фотографии. Но зачем это знать посторонним людям?

1. Получили новый паспорт, водительское удостоверение? **Не публикуйте фото с документами,** где видны их данные. Это же касается билетов на самолет.
2. **Не пересылайте и не храните в соцсетях и мессенджерах документы, пароли, коды, реквизиты карты и счетов.** Это очень чувствительные данные.
3. Не рекомендуется входить и **авторизироваться на сторонних сайтах через учетную запись соцсети.** Не всегда перед входом можно проверить ”надежность“ ресурса, а это, в свою очередь, чревато тем, что страницу могут украсть.
4. **Настройте уникальные и надежные пароли** для всех своих учетных записей. Использование одних и тех же многократно подвергает их риску.
5. Используйте проверенные **антивирусные службы и лицензионное программное обеспечение.**

Помните, информация, оставленная в социальных сетях, – это зачастую навсегда. Прежде чем публиковать очередной пост или что-то писать в комментариях, необходимо подумать, проверить и убедиться в необходимости такой публикации. И хотя всегда можно удалить нежелательные сообщения, вы не знаете, кто собрал эту информацию и ваши персональные данные раньше и что с этими данными собирается сделать потом, в том числе, возможно, использовать против вас.



**ГУК «Смолевичская центральная районная библиотека**

**имени Максима Богдановича»**

**Отдел обслуживания и информации**

**СПОРИМ, Я ЗНАЮ О ТЕБЕ ВСЁ? ПЕРСОНАЛЬНЫЕ ДАННЫЕ В** **ИНТЕРНЕТЕ**

 **(Буклет)**



**(Буклет)**

**г. Смолевичи, 2024 год**

 **Страницы в соцсетях, куда вы добровольно выкладываете личную информацию и фотографии, смотрят не только друзья, но и мошенники, для которых интернет является безграничным источником сведений о вас.**

**Как это работает?**

Вот несколько примеров:

* Фото из отпуска оповещают, что вас нет дома.
* Хвалебные посты о дорогостоящих покупках сориентируют других на предмет вашего финансового состояния.
* Метка геолокации на фото в соцсети, сделанном по месту проживания, позволяет установить дом, в котором живет лицо, опубликовавшее фотографию.
* Размещая личный номер мобильного телефона или электронной почты в сетях, вы рискуете получить шквал ненужных вам звонков, сообщений, рассылок с рекламными предложениями, а можете попасться «на удочку» аферистов.

**Важные правила БезОпасности**

Немного о базовых правилах безопасного оборота ваших персональных данных в социальных сетях:

1. **Читайте политику конфиденциальности соцсети.** Важно знать, кто будет обрабатывать ваши персональные данные, как хранить и использовать.
2. Делитесь сокровенными моментами своей жизни только с близкими, а для этого **уделите внимание настройкам конфиденциальности в соцсетях**, попросту закройте страницы. В настройках профиля есть раздел ”Приватность“. В нем вы можете ограничить круг тех, кто сможет писать вам сообщения, оставлять комментарии или видеть основную информацию вашей страницы. Следуйте правилам безопасности, если вы решили оставить профиль открытым и видимым для вех.
3. Установите в соцсетятях и мессенджерах **двухэтапный вариант проверки**, который позволяет создать персонализированный PIN-код для большей безопасности от нарушений и хакеров.
4. **Не публикуйте в открытом доступе избыточную информацию**: адреса, номера телефонов, даты рождения. Это же касается и сведений о родных и близких, не публикуйте чужие фото и видео (даже совместные) и иную личную информацию **без согласия** на то человека. Вы просто не имеете на это права.
5. **Не используйте геолокацию**, когда размещаете в соцсетях фото дома, не отмечайте на нем адрес. Зачастую по умолчанию к каждому снимку, который вы делаете, привязывается местоположение. Оно сохраняется в метаданных изображения.