ЦИФРОВОЙ СЛЕД

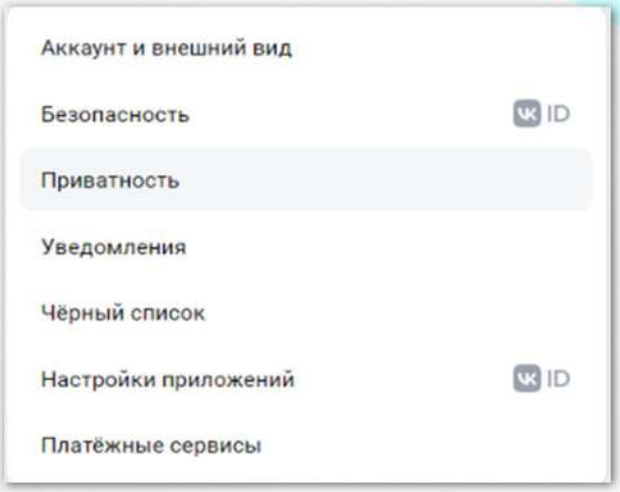
Цифровой след — это совокупность данных, которые мы оставляем о себе в интернете в процессе онлайн-активности

Он включает в себя посты в социальных сетях, комментарии, поисковые запросы, данные о местоположении и информацию, собираемую на сайте (так называемые cookies).

Цифровой след важен, поскольку он может влиять на вашу личную безопасность,репутацию, а также он используется для показа рекламы лично для вас.

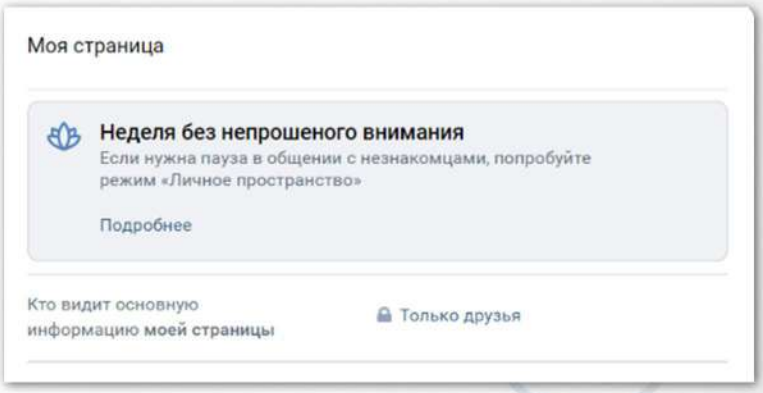
Цифровой след является целью многих хакеров, его используют для шантажа, вымогательства, взлома и других преступлений.

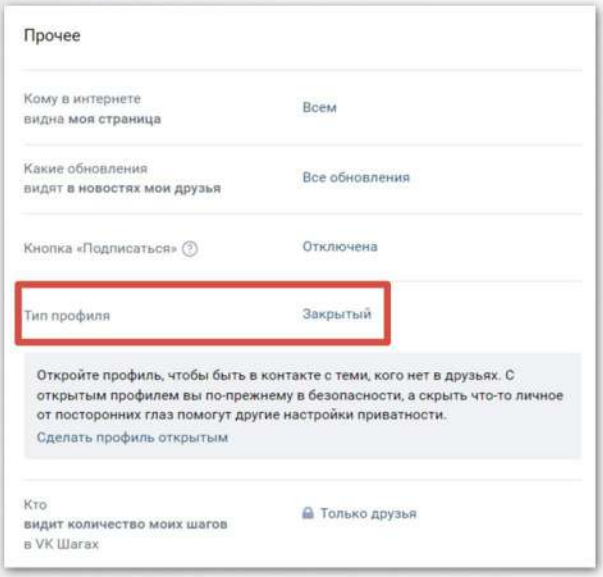
Разберем, как обезопасить свой цифровой след от злоумышленников



Начнем с социальных сетей. У каждой из них есть настройки, позволяющие контролировать, кто видит вашу информацию.

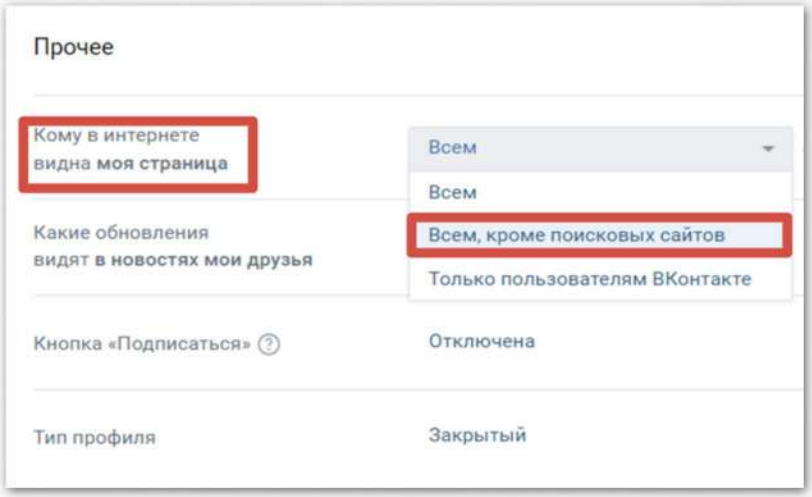
Рассмотрим на примере социальной сети VK. В настройках перейдите в раздел «Приватность».



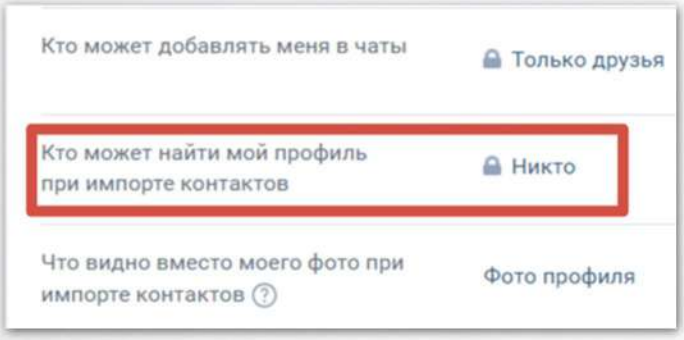


В разделе «прочее» скройте свой аккаунт от посторонних глаз, с помощью пункта «Тип профиля». С помощью этой настройки вы сможете защитить свою страницу от посторонних, они не увидят информацию о вас и о ваших друзьях.

Если ваш профиль зарегистрирован под настоящими именем и фамилией, то его можно найти через поисковые системы, такие как Google или Yandex.

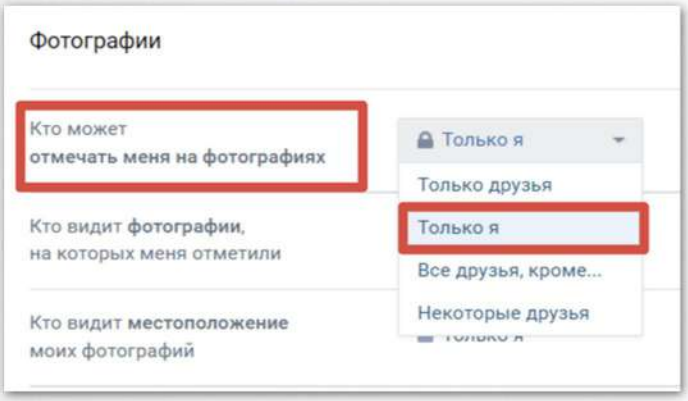


К счастью, VK позволяет это изменить, запретите в настройках приватности, в разделе «Прочее» доступ поисковых систем к вашему аккаунту.



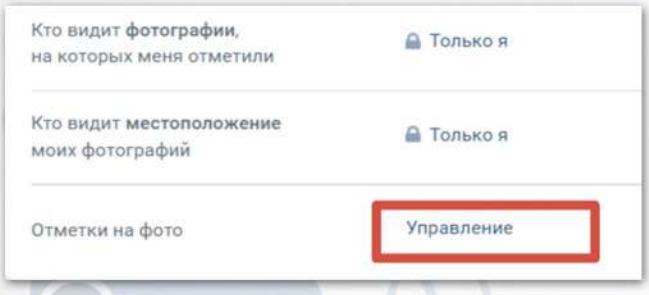
В настройках приватности найдите раздел «Связь со мной», найдите пункт «Кто может найти мой профиль при импорте контактов», переведите настройку в режим «Никто».

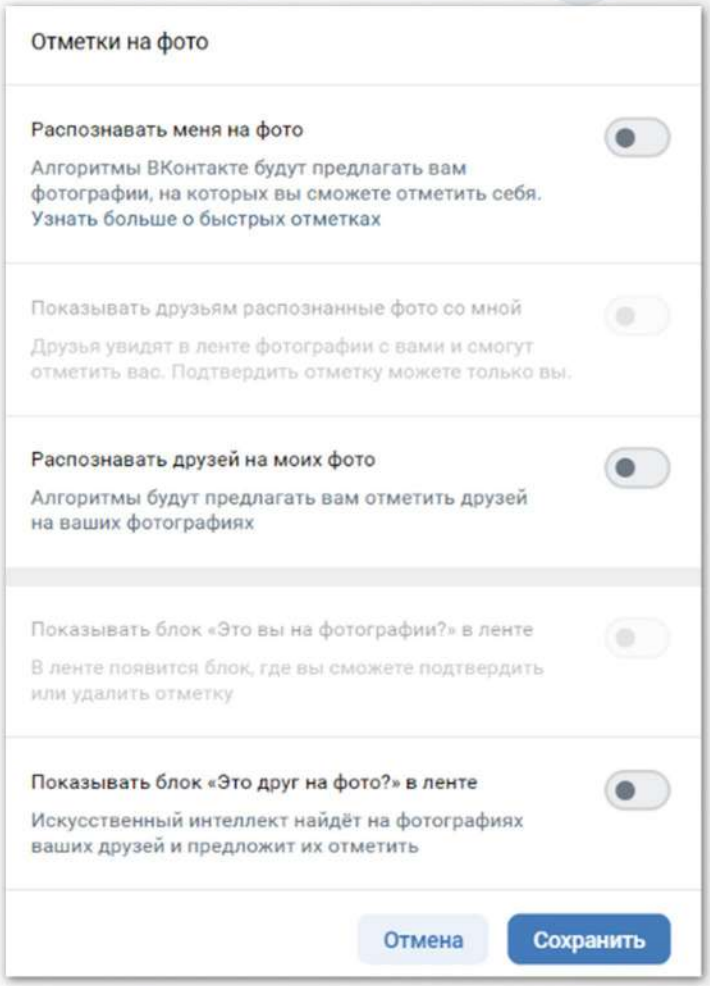
Таким образом вы снизите вероятность, что вас найдет кто-то, в чьих контактах записан ваш номер. Также вы снизите вероятность попадания вашего профиля в рекомендации других пользователей.



В разделе «Фотографии» выберите пункт «Кто может отмечать меня на фотографиях» и переведите его в режим «Только я», так вы усложните поиск злоумышленников информации о вас.

В этом же разделе вы можете настроить алгоритмы распознавания вашего лица в пункте «Отметки на фото», нажав на кнопку «Управление».





Это основные рекомендации по настройкам приватности в Вконтакте, помимо них существуют и другие настройки. Просмотрите их и выберите наиболее безопасные для вас.

Отталкивайтесь от того, что это вы должны искать что-то в социальных сетях, а не о вас должны искать информацию. Аналогично вы можете настроить и другие социальные сети.

Перед публикацией каких-либо материалов подумайте, хотите ли вы чтобы их видели посторонние? Не содержится ли там ваша личная информация? Может ли что-то извлечь злоумышленник из этой публикации?

Также не стоит выкладывать провокационные публикации или что-то, что может навредить вашей репутации.

Помните - все, что вы делаете в интернете, оставляет след.

Удаляйте неиспользуемые аккаунты и контент на различных сайтах.
Чем меньше информации в интернете о вас (даже неактуальной), тем сложнее злоумышленнику будет искать о вас информацию.

В настройках мобильных приложений установите ограничения доступа к вашим данным.
Это может быть доступ к вашему местоположению, вашей камере, вашей фотогалерее. Также стоит удалять приложения, которые больше вам не нужны.

Старайтесь не использовать публично доступные Wi-Fi-сети.
Все, что вы делаете вы интернете, видно владельцу этой сети.

Не используйте одинаковые ники в различных соц. сетях, мессенджерах. Например, неправильно использовать имы почты example@mail.ru, имя социальной сети https://vk.com/example и имя в Telegram @example.
Зная всего один ник, злоумышленник сможет понять какие профили принадлежат вам. Это упростит его работу.

Сейчас актуальны атаки, когда злоумышленники ищут сотрудников конкретных организаций и выманивают у них деньги.

Указывая место работы в социальных сетях и других сайтах, маскируйте название компании.

Например, вы работаете в ООО «Альфа». Замените русские буквы «а» на латинские. У вас получится ООО «Aльфа» - выглядит как оригинальная надпись, но зато вас не смогут найти через поисковые системы, как сотрудника этой организации.

Аналогично вы можете менять буквы и в других интернет-сервисах.

Например, в компании по доставке еды, в фамилии Иванов, буквы «а» и «о» можно заменить. После того, как в этой компании произойдет утечка, вас не смогут найти по фамилии.

С пожеланиями безопасности, StopPhish