

Содержание

- мне нечего скрывать** 3
 - Если мне нечего скрывать, то мне нечего бояться 3
 - Я никому не нужен 3
 - Всё и так известно 3
 - Защита - общее дело 4
 - Что делать? 4
 - Доп.материалы 4

мне нечего скрывать

[eff_anniversary.mp4](#)

Если мне нечего скрывать, то мне нечего бояться

Я - законопослушный гражданин, мне нечего скрывать - С тем, что ты законопослушный гражданин, можно поспорить, даже если ты не ищешь, как бы сделать бомбу из хозмага. Все люди постоянно нарушают какие-либо законы и правовые акты, даже не зная об этом.

Даже если у тебя нет криминальных намерений, это не означает, что ты хочешь делиться всеми своими личными данными. Если я предложу тебе выложить в публичный доступ сканы, фотографии, данные биометрии, все архивы документов, логины и пароли, список контактов, все переписки, записи телефонных разговоров, - ты откажешься, ты уже скрываешь свои данные. Почему?

Я никому не нужен

Я никому не нужен, зачем кому-то за мной следить - Это распространенное заблуждение.

На самом деле, за тобой уже следят и собирать данные. Даже если ты не представляешь интереса для кого-либо лично, ты - часть больших общностей, контроль над которыми - предмет интереса множества лиц и организаций. Коммерческие структуры и государства собирают информацию для маркетинга, контроля и репрессий.

За тобой могут целенаправленно следить, даже если ты не представляете никакого интереса, а им нужны данные о ком-то из твоего круга общения.

В мире, где подовляющее число людей смотрит на свои смартфоны как на волшебные зеркальца - слежка, увы, современная действительность. Под лозунгами «за все хорошее», «удобства ради» все чаще делаются самые страшные вещи.

Всё и так известно

Государство и злоумышленники всё и так знают - Далеко не всё. Много, но далеко не всё. К тому же, в твоих силах сделать так, что бы твое цифровое досье больше не пополнялось.

Они знают только то, что ты им предоставил. Иных способов сбора данных о тебе у них, в контексте массовой слежки, попросту нет. И только в твоих силах этому противодействовать. Да даже противодействовать не надо. Просто нужно лишний раз не светить своими персональными данными.

В современном мире и плотном вхождении технологий в обычную жизнь, интернет становится не средством коммуникации, а оружием массового поражения в умелых руках, направленным против тех кто не заботится о своей безопасности.

Защита - общее дело

Почему защита личных данных - это общее дело?

Человек социальное существо. Наплевательским отношением к хранению и распространению приватной информации ты вредишь, да именно вредишь, не сколько себе, а еще своему окружению и обществу в целом. Ты ставишь под угрозу безопасность других лиц, ставя чужое право на неприкосновенность частной жизни под удар.

Тут важна массовость. Это крайне усложнит попытки злонамеренного доступа к твоим данным и вообще любой информации о тебе и твоём круге общения от злонамеренного использования, политических преследований, манипуляций твоим мнением. Усложнит слежку и контроль над информацией, мнениями, людьми. Все это преследует одну простую цель - избежать превращения мира в цифровую антиутопию, к которой он летит на всех парах.

Что делать?

Следует придерживаться простых правил:

- Если технически данные возможно скрыть, нужно их скрыть. Относится это к любым данным вплоть до местоположения, ip адреса, и прочих разрешений экрана.
- У каждого сотового телефона есть уникальный IMEI-код. Когда ты вставляешь в него сим-карту, этот код регистрируется в базе сотового оператора и таким образом закрепляет прямую связь между владельцем номера телефона и владельцем аппарата.
- Избегать сервисов занимающихся слежкой за пользователями и собирающих личные данные для любых целей. Проприетарный софт - черный ящик, соответственно использовать windows, osx, ios, android и тп - нельзя.
- Использовать стойкое оконечное (end-to-end) шифрование для приватных¹⁾ переписок. Чтобы исключить техническую возможность подмены данных или перехвата их любыми третьими лицами.
- Не плати везде банковской картой, максимально используй наличные для мелких сиюсекундных трат. Любая транзакция фиксирует твоё точное месторасположение.
- Любое место, где ты предъявляешь документы - фиксируют это. Используй поддельные / чужие документы.
- Никогда не пользуйся авторизацией через биометрию и не оставляй ее нигде!

Это минимальные требования цифровой гигиены в современном мире.

Доп.материалы

[pgrgu](#)

["Шифропанки: свобода и будущее интернета"](#)

¹⁾

И абсолютно не имеет значение доверяешь ли ты сервису предоставляющему услуги или нет. Сервис может быть просто взломан или принужден к противозаконным действиям. А твои данные попадут отнюдь не в хорошие руки. А вышеописанные меры защитят тебя от таких утечек.

From:

<https://wiki.radi0.cc/> - **radi0wiki**

Permanent link:

https://wiki.radi0.cc/worldly:nothing_to_hide

Last update: **2025/11/09 12:07**

