

Как следит за вами телевизор и почему тесты в соцсетях проходит опасно, рассказывает известный эксперт по ИТ-безопасности Игорь Ашманов.

– Говорят, что вся техника с камерами – ноутбуки, планшеты, телефоны – следит за нами, снимает фото и видео, когда ей вздумается. Это правда?

– Да. Не зря Марк Цукерберг, основатель сети «Фейсбук», технически очень продвинутый человек, заклеивает камеру на своем ноутбуке скотчем – и начал делать это еще 7 лет назад! Ваш телефон всегда вас «слушает», всегда определяет ваше местоположение и постоянно смотрит в камеру на вас – даже когда, казалось бы, не активен. При этом телефон понимает, если снимок сделан в кармане, и на экране темно. Снимки же с лицами, людьми, какими-то ситуациями аппараты отправляют на «центральные сервера». Кто выгодоприобретатели этой информации, – можно только предполагать... К данным с аппаратов с ОС «Андроид» имеют доступ не только производители телефона, но и АНБ, которому владелец ОС обязан отдавать данные по закону.

– Выходит, нужно выключать телефон, когда им не пользуешься?

– Это не поможет. Надо понимать, что каналов слежки много. Надо стараться не совершать ничего компрометирующего. Потому что, даже если вы считаете, что телефон выключен, далеко не факт, что это так. Гарантия отключения – съем батареи с аппарата. Почти все современные телефоны имеют несъемную батарею. С выключением тоже не все просто: аппарат может проигрывать вам анимацию выключения и гасить экран, но оставаться активным. Есть другой вариант, как усложнить слежку: купить «бабушкофон» вроде «Нокии-6610» и не пользоваться смартфонами.

– Вы известный эксперт в области цифровой безопасности – покажите, а какой у вас телефон?

– Я не эксперт, извините. У меня один из последних корейских смартфонов. И камера

не заклеена, вот, смотрите. Прослушка и слежка несет непосредственный риск для людей, которые имеют дело с какими-то тайнами. Это чиновники, представители спецслужб, крупные бизнесмены и преступники. Сервера же собирают массивы данных, не выделяя из них конкретно меня как личность (пока). Скорее всего, производитель телефона и АНБ не следят за личными перипетиями моей жизни. В любом случае я стараюсь не использовать телефон в специфических ситуациях: на переговорах, в сауне, спальне и т. п.

– То есть бояться, что чья-то жена узнает об измене, потому что за мужем следит телефон, не стоит?

– Ну у жены обычно нет доступа к данным, которые смартфон отправил в США. Жене проще взять мужнин смартфон и прочитать, о чем и с кем он там переписывается. А вот тем спецслужбам, которые собирают данные, шантажировать мужа, конечно, можно. Если муж того стоит (он большая шишка, например).

– Говорят, мессенджеры («Телеграм», «Вотсап», «Вайбер») шифруют информацию. И в отличие от смс и электронной почты они безопаснее. Это так?

– Не уверен. Этого никто не может знать доподлинно. Это же маркетинг. Надежный ли алгоритм шифрования, на чьих серверах и в каком виде хранится ваша переписка? Простой пример: знаете, что публичная почта (например, «Гугла») «читает» содержимое ваших писем? Она предлагает вам рекламу того, о чем шел разговор в письмах. А «Гугл» по закону обязан отдавать данные разведке. Аналогично устроены все коммуникационные сервисы: конечно, читают не живые люди, а искусственный интеллект с лингвистическим анализом. А операционная система Windows-10 в изначальной поставке имеет встроенного клавиатурного шпиона, который все ваши нажатия клавиш отправляет в «Майкрософт».

– Многие выкладывают в соцсети фото детей, отмечают свое местонахождение – насколько это безопасно?

– В нашей семье был такой опыт: у жены похитили сына. Все кому не лень тогда сообщали, что он выкладывал о себе все в соцсетях. И хотя это было не так, а сына

украли по наводке, мы к информации о детях в цифровом пространстве относимся крайне нервно и дочерям подобного не позволяем. Если в сети можно посмотреть, как выглядят наши дети и где они бывают — это значит, потом их можно будет узнать на улице, в парке, песочнице.

– В соцсетях постоянно расшаривают тесты: каким вы будете в старости, какая вы собака... При этом для получения результата нужно предоставить доступ к данным профиля. Это безопасно?

– Выкачать публичный профиль можно и внешними программами. Опасность тестов, на мой взгляд, в другом. Это массовая дрессировка людей, натаскивание их на выполнение чего-то по команде. Механизм прост: большинству людей не хватает внимания к себе, а тут им говорят, что ты талантливый кулинар или похож на знаменитость. Приятно! Какое ты животное, кем ты был в прошлой жизни – миллион идиотских результатов, которыми все делятся с друзьями. Дрессировка состоит именно в «поделиться». Такой же смысл несут флешмобы: облей себя водой или напиши, как тебя изнасиловали. Так тренируют бездумное массовое поведение, как у леммингов. Мне говорят – я делаю: все побежали, и я побежал. Тот, кто собирает массовые данные, ставит пометку: вот эти пользователи склонны вестись на массовые действия. Работа такая же, по сути, как в «группах смерти» (которые далеко не самое страшное, что сейчас есть в Сети). Дрессированным массам людей можно подкидывать задания все сложнее, и они охотно их выполняют.

– Вы сказали, есть что-то страшнее «групп смерти». Что?

– Группы блатной романтики АУЕ, группы романтизации школьных расстрелов (по-английски «скулшутинга»). На самом деле вот такая кибербезопасность должна волновать и семью, и государство в первую очередь. Когда пароль украли – это полбеда. А вот когда украли мозги – это гораздо хуже. Манипуляторов в сети сейчас тысячи, и они становятся все изощреннее. Проверяйте, чем занимаются в Интернете ваши дети, в каких группах и с кем они общаются, какие задания выполняют – это может спасти им жизнь.

(www.aif.ru)