Скажи личным тайнам -

прощай!

С появлением глобальной сети интернет защита информации стала одной из главных проблем, с которой столкнулась цивилизация. На 80% информация сегодня беззащитна. Пользователи сами открывают доступ к своим аккаунтам в социальных сетях, к своей почте и т. д. Оказывается, наши следы в интернете, проанализированные специальной программой, могут сообщить о нас уникальную информацию!

Информация никуда не исчезает?

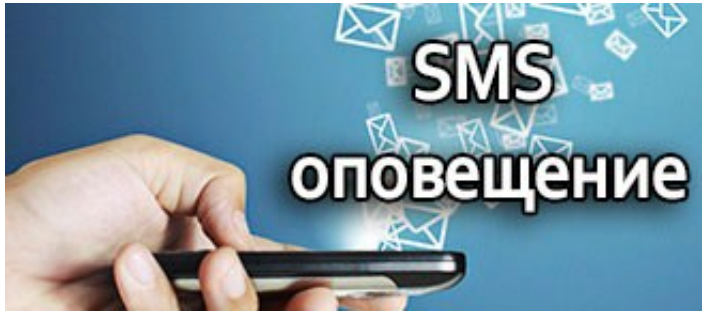
Сегодня человек, делая селфи, активно фотографирует себя, выкладывает это в Вконтакте, в Фейсбуке и других соцсетях. А ведь через 20 лет может случится так, что вегетарианство станет мейстримом (банальщина и избитость, «то, что делает большинство»), и ваша фотография в ресторане с жареными рёбрышками окажется компрометирующей информацией…

Таким образом, люди, которые вовремя найдут и проанализируют эту информацию, станут для вас опасными.

Несколько лет назад 14-ти летняя американская девочка очень активно пользовалась скидочной картой в одном гипермаркете. Спустя некоторое время ей на почту стали приходить рекламные буклеты товаров для беременных. Это попало на глаза отцу. Он оскорбился, подал в суд на магазин. Но выяснилось, что девочка на самом деле была беременна, причём сама об этом не знала. Все думали, что работники присылали эти буклеты, а оказалось, что об этом узнала программа, проанализировав изменившиеся предпочтения девочки. Она перестала покупать прокладки, начала приобретать много солёного, больше сладкого. И робот, поняв, что такое поведение свойственно беременным, начал ей высылать рекламные буклеты.

Во всём этом есть и удобства. Какие?

К примеру, заходите вы в кафе в Санкт-Петербурге, покупаете чашку кофе и булочку , после этого расплачиваетесь специальной программой, стоящей на смартфоне. Через 3 часа к вам на телефон приходит уведомление: такое же кафе находится в 300 метрах от вас. Это достаточно удобно, и большинству людей это нравится.



Основные правила защиты от взлома

Ставьте сложные и, самое главное, разные пароли на все хранители информации. НАДЕЖНЫЙ пароль — не менее 8 символов, включая заглавную букву и цифру

Пользуйтесь антивирусом со свежими базами

Не посещайте сомнительные сайты!

Не открывайте письма от неизвестных адресатов