4.

ЗАМЕТАЕМ СЛЕДЫ

Браузер на вашем телефоне хранит много личной информации – ваше местонахождение, запросы в поисковике, использованные веб-сайты – и может ее распространять. Вы в силах это контролировать, выполнив несколько действий.

Как правило, телефоны, планшеты и компьютеры мы получаем с предварительно установленными браузерами, которые не заботятся о вашей конфиденциальности. Вместо них вы можете скачать и использовать другой браузер, который по умолчанию обеспечивает конфиденциальность ваших действий в сети, защищая вас от трекеров.

Для дополнительной защиты от отслеживания вы можете подключить дополнения и расширения (add-ons and extensions) – простые в установке мини-программы для браузера, которые сделают вашу онлайн-активность более приватной.

5.

УБЕРИТЕ МЕТКИ

Участвовали в сборе данных о ваших друзьях, отмечая их на фотографиях и в публикациях?

Облегчите их груз данных (и свою совесть, в том числе), по возможности убрав упоминания о них на как можно большем количестве фотографий и публикаций.

Передайте дальше! Мотивируйте своих друзей, семью и коллег присоединиться к вам в контроле за улетучивающимися данными. Прилагая усилия к защите личной информацию, мы сможем помочь друг другу в процессе «детокса».

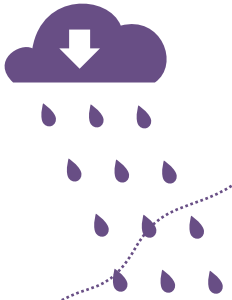
Проект создан

TACTICAL TECH

При поддержке

Firefox

datadetoxkit.org
#datadetox



DATA DETOX KIT

Для блокировки шпионской рекламы и невидимых трекеров установите uBlock Origin (для Chrome, Safari и Firefox) или Privacy Badger (для Chrome, Firefox и Opera).

Чтобы убедиться, что ваше подключение к сайтам максимально безопасно, установите опцию HTTPS Everywhere: расширение браузера, гарантирующее защиту и зашифровку персональных данных во время пользования большинством веб-сайтов. Если вы пользователь Safari, выберите в качестве поисковой системы продукт, не принадлежащий Google (например, DuckDuckGo), который автоматически будет перенаправлять вас на зашифрованное соединение.

КОНТРОЛИРУЙТЕ ДАННЫЕ СВОЕГО СМАРТФОНА

чтобы сохранить конфиденциальность в сети

Если прикинуть, о чем ваши данные говорят другим, то это может показаться чепухой: кого волнует, что вы поклонник кантри, любите покупать много обуви или планируете свой отпуск на год вперед?

Однако проблема в том, что происходит с вашими данными – со временем они формируют персональную цифровую модель: ваши привычки, передвижения, отношения, предпочтения, убеждения и секреты становятся видимыми для тех, кто анализирует и извлекает из них выгоду (например, большие компании или информационные брокеры).

С помощью программы «Цифровая детоксикация» вы поймете, как и почему это происходит, и предпримете практические меры для контроля ваших данных в интернете.

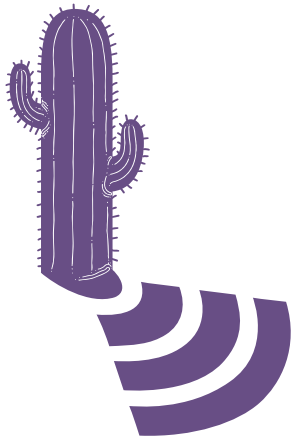
Поехали!

1.

ПЕРЕИМЕНУЙТЕ УСТРОЙСТВО

В какой-то момент вы дали своему телефону имя для подключения к Wi-Fi и Bluetooth, или, возможно, гаджет получил название автоматически, во время настройки. Это значит, что «Телефон Алекса Чанга» видит владелец сети Wi-Fi; если у вас работает Bluetooth, его видят все люди в вашем радиусе, у которых он также включен.

Вы бы не стали объявлять свое имя, заходя в кафе, ресторан или находясь в аэропорту. Телефон также не должен этого делать.
Выберите имя телефона, не позволяющее вас идентифицировать, но которое будет уникальным для вас.
Как это сделать:



iPhone:
Изменить имя телефона:
Настройки → Основные → Об этом устройстве → Имя

Android:
Изменить название Wi-Fi:
Настройки → Wi-Fi → Меню → Расширенные настройки / Дополнительно → Wi-Fi Direct → Переименовать устройство
Изменить название Bluetooth:
Настройки → Bluetooth → Включите Bluetooth, если он выключен → Меню → Переименовать устройство → Выключите Bluetooth

2.

УДАЛИТЕ ИСТОРИЮ МЕСТОПОЛОЖЕНИЙ

На первый взгляд может показаться, что данные о вашем местоположении – просто незначительные порции информации. Но собранные вместе, они могут раскрыть ваши тайны и привычки, например, где вы живете, работаете, где любите встречаться с друзьями. Эта функция пользуется большим спросом у многих компаний и информационных брокеров.

Вы можете отключить определение локации в настройках приложений. Для начала подумайте, какие приложения не требуют его для работы (действительно ли этой игре нужно знать, где вы находитесь?) и от каких вы бы хотели его скрыть:

Android:
Настройки → Приложения → Местоположение

iPhone:
Настройки → Конфиденциальность → Службы геолокации → Управление

3.

ПОЧИСТИТЕ ПРИЛОЖЕНИЯ

Приложения социальных сетей, игры и мобильный прогноз погоды – все заинтересованы в ваших данных... и собирать их они могут довольно долго.

Удалите ненужные приложения с вашего телефона, это хороший способ детоксикации вашего цифрового «я».

Кроме того, такая чистка телефона освободит место, уменьшит потребление данных и увеличит время работы аккумулятора.

Android:
Настройки → Приложения → Выберите приложение, от которого желаете избавиться → Удалить

iPhone:
Найжмите и удерживайте значок одного приложения, пока все не начнуть мигать и в верхнем левого углу каждого не появится крестик.
Для удаления приложения нажмите крестик на его значке.
Чтобы вернуться к обычному виду, нажмите на кнопку «Домой».

4.

ЗАЩИТИТЕ СВОИ ВИРТУАЛЬНЫЕ ЦЕННОСТИ

Информация в вашем телефоне нуждается в такой же заботе, как и ценные вещи в доме – финансовые отчеты, сканы паспорта или даже ваш адрес и номер телефона. Стоит подумать, где вы храните свои **ценные личные данные** и как можете их защитить.

Точечная чистка идеально подходит, чтобы сделать что-то полезное за чашечкой кофе. Вспомните о той информации, которая содержится в вашей электронной почте или в других аккаунтах – скан удостоверения личности, банковские реквизиты или данные медицинской страховки – и удалите ее. Если эти данные понадобятся вам позже, скачайте или распечатайте их перед ликвидацией из вашей учетной записи.

Глубокая чистка более тщательна, и ее следует делать раз в год. Заархивируйте все письма в электронной почте или аккаунте в социальных сетях, загрузите архив на свой компьютер и удалите содержимое учетной записи, начиная все с чистого листа.

Совет: не просто удаляйте — очистите также корзину и временные файлы!

Вам решать, создавать ли резервную копию своих архивов и документов в облаке, хранить их на переносном жестком диске или USB-накопителе. Независимо от того, где и как вы храните информацию, убедитесь, что не потеряете ее и защитите надежным и понятным вам паролем.

5.

ПОДУМАЙТЕ О БЛИЖНЕМ

Мы часто забываем, что интернет неспроста называется «паутиной». Так или иначе, мы все связаны друг с другом: не как «друзья» в социальных сетях, но и с помощью контактов в учетных записях электронной почты и фотографий, которыми делимся онлайн. Защищая свои учетные записи, усильте пароли и удалите личные данные. От этого выиграете не только вы – все связанные с вами контакты также получат дополнительную безопасность.

Очищая электронную почту и социальные сети, подумайте, что еще вы можете скачать или удалить, как это может помочь вашим друзьям или коллегам: банковские реквизиты сестры, код доступа к офису или скан паспорта ребенка – все это может создать проблемы, попав не в те руки.

Расскажите об этом! Для усиления цифровой безопасности достаточно нескольких шагов. Поделитесь информацией о «Цифровой детоксикации» с друзьями, семьей и коллегами, чтобы помочь им изменить свои привычки и защитить ценные для них вещи.

DATA DETOX KIT

НА СТРАЖЕ НАСТРОЕК

для защиты персональных данных

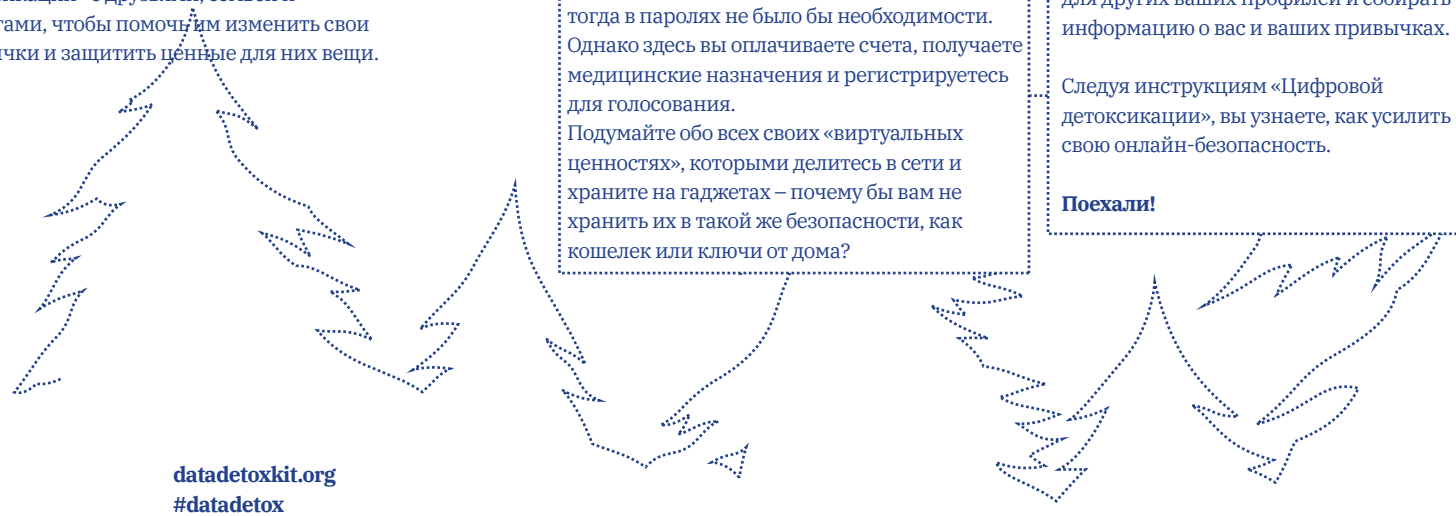
Если бы в интернете просто обменивались изображениями собак в костюмах динозавров, тогда в паролях не было бы необходимости. Однако здесь вы оплачиваете счета, получаете медицинские назначения и регистрируетесь для голосования.
Подумайте обо всех своих «виртуальных ценностях», которыми делитесь в сети и храните на гаджетах – почему бы вам не хранить их в такой же безопасности, как кошелек или ключи от дома?

Есть один простой способ усложнить другим доступ к виртуальным ценностям: не давайте им возможности угадать ваш пароль. Большинству людей не нужны специализированные технические навыки, чтобы войти в чужой аккаунт, они могут сделать это, угадывая комбинации цифр и букв или с помощью автоматизированной программы.

Как только они получают доступ к одному аккаунту, то будут подбирать этот пароль для других ваших профилей и собирать информацию о вас и ваших привычках.

Следуя инструкциям «Цифровой детоксикации», вы узнаете, как усилить свою онлайн-безопасность.

Поехали!



Проект создан
TACTICAL TECH

При поддержке
Firefox

datadetoxkit.org
#datadetox

1.

ЗАПРИТЕ СВОЮ ЦИФРОВУЮ ДВЕРЬ

Блокировка экрана паролем или графическим ключом, доступ к телефону с помощью отпечатка пальца или идентификатора лица – одни из лучших способов против того, кто захочет влезть в чужой гаджет. Есть много средств защиты, и иногда трудно понять, какое из них подходит именно вам.

Наличие блокировки на телефоне, планшете или компьютере всегда лучше, чем ее отсутствие. Как и разные типы дверных замков, некоторые виды блокировки экрана надежнее других.

Длинные и уникальные пароли – самые надежные, такой пароль должен содержать **буквы, цифры и специальные символы.**

Допустим, что для разблокировки смартфона вы используете стандартный свайп. Можно усилить защиту, установив длинный пароль. Или вы используете графический ключ? Тогда сделайте рисуок длиннее! Используете комбинацию цифр 1234 как PIN-код? Бросьте игральные кости семь раз подряд и запомните выпавшие числа как новый PIN-код. **Небольшие изменения могут сыграть большую роль в защите вашего устройства.**

2.

СИСТЕМА ДОСТУПА

Создавать первоклассные пароли легко, нужно только следовать нескольким основным принципам. Ваши пароли должны быть:

Длинными: **состоять минимум из восьми символов. А 16-20 знаков еще лучше.**

Уникальными: **выбирайте для каждого сайта разную комбинацию символов.**

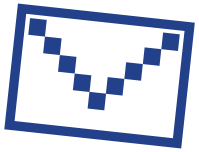
Случайными: **они не должны иметь логических объяснений или легко угадываться. Тут на помощь придут менеджеры паролей.**

Самый надежный пароль состоит из комбинации букв, цифр и специальных символов. Этот проверенный временем способ до сих пор усложняет мошенникам работу. К сожалению, некоторые системы не разрешают использовать такие специальные символы, как @ # $% - = +. Но достаточно длинная комбинация букв и цифр по-прежнему лучше короткой.

В идеале, используйте специальную систему для создания и хранения всех ваших паролей. Специалисты по безопасности часто рекомендуют сервисы вроде 1Password и KeePassXC. Единственная цель этих приложений – защитить ваши учетные данные и другую конфиденциальную информацию.

3.

ДОБАВЬТЕ ВТОРОЙ КЛЮЧ



Настройка двухфакторной (2FA) или многофакторной аутентификации (MFA) означает, что даже если кто-то разгадает ваш пароль, то, скорее всего, не узнает дополнительный и необходимый ключ.

Посмотрите в настройках безопасности наиболее используемого сайта или приложения, можно ли добавить дополнительный ключ. Начните с самых важных: финансовых приложений или электронной почты, которую вы используете для восстановления других учетных записей.

Google:
Войдите в свой аккаунт: myaccount.google.com → Безопасность → Двухэтапная аутентификация → Начать

Facebook:
Меню → Настройки → Безопасность и вход → Использовать двухфакторную аутентификацию

Совет: При настройке дополнительного уровня проверки вам нужно выбрать второй способ подтверждения вашей личности. Старайтесь не использовать SMS (текстовые сообщения, отправленные на ваш номер телефона) в качестве второго фактора – на случай, если потеряете мобильный.

4.

ЗАЯВИТЕ О СЕБЕ

Если вам не нравится зависимость от используемых приложений или навязчивая дезинформация на часто посещаемых сайтах, вы можете высказать свое мнение, отправив электронное письмо, написав твит. Таким образом вы сообщите компаниям, что не согласны с их политикой. Пользователи являются самым ценным активом интернет-компаний, и подобные отзывы повышают шансы на то, что они могут изменить свою практику.

Если вам кажется, что ваш отзыв не услышан, есть другое эффективное средство: использовать другой сайт или приложение. Если вы сообщите о своем недовольстве сайтом или приложением, а потом перестанете им пользоваться, и так поступит еще достаточное число пользователей – **компании это заметят.**

5.

ГОВОРИТЕ ОБ ЭТОМ

Распространяйте информацию! Этот совет легко забыть, однако он может быть очень эффективен. Поделитесь со своими друзьями, семьей, коллегами своими наблюдениями и даже попросите их присоединиться к вам в детокс-марафоне! Все борются со своими телефонными зависимостями. Важно найти способ, который подходит именно вам и соответствует вашему образу жизни. Поэкспериментируйте, пока не найдете подходящий вариант, а со временем обновляйте привычки по мере изменения потребностей. Помните, что универсального решения не существует.

И, наконец, предупредите о новом цифровом поведении окружающих. Например, что ежедневно после 8 вечера вы недоступны в мессенджерах, потому что с этого времени начинается ваша жизнь без смартфона. Расскажите об этом семье и друзьям, чтобы в случае необходимости они могли связаться с вами другими способами. Поддерживайте диалог, задавайте вопросы – и вы сможете жить сбалансированной онлайн-жизнью, которая подходит именно вам.

DATA DETOX KIT

ОТКАЖИТЕСЬ ОТ ПРИВЫЧКИ

для улучшения вашего цифрового благополучия

Как давно вы отключались от сети и не касались гаджетов в течение всего дня или хотя бы часа? Если вы постоянно онлайн, знайте: вы не одиноки. Как вы можете быть уверены, что проводите время в смартфоне с пользой?

Отметим, что непреодолимая тяга к гаджетам – это не ваша вина! Верите или нет, но все ваши любимые приложения и веб-сайты разработаны таким образом, чтобы каждая функция, цвет и звук были «оптимизированы» и держали вас на крючке. Компании заинтересованы в продажах и в том, чтобы пользователь всегда возвращался за еще большей порцией контента.

Хотите найти баланс между своей онлайн и оффлайн жизнью? Это и является целью «Цифровой детоксикации».

Поехали!

Проект создан
TACTICAL TECH

При поддержке
Firefox

datadetoxkit.org
#datadetox

1.

ЖИВИТЕ ЗДЕСЬ И СЕЙЧАС

Этот совет сложнее, чем кажется на первый взгляд. Пребывание в моменте требует ежедневной практики. Это что-то вроде мышцы в мозге, которую нужно регулярно тренировать для укрепления своей силы. Можете начать с отслеживания своих отношений с технологиями.

Сколько времени вы проводите в смартфоне?

Если вы недовольны ответом, ниже есть настройки и стратегии, которые помогут вам получить контроль над вашими устройствами.

Если ваша цель – проводить меньше времени в Facebook, Instagram или Snapchat, измените настройки и позвольте этим приложениям работать на вас.

Некоторые приложения, как Instagram, даже позволяют установить дневной лимит использования и напоминают о его достижении.

Instagram:
Профиль → Меню → Настройки → Аккаунт → Ваши действия → Установить ежедневное напоминание

Если вы замечаете, что телефон мешает работе постоянными сообщениями, звонками, гудками или сигналами, можно временно отключить оповещения, перевернуть его экраном вниз или даже спрятать в сумку или карман, чтобы он не попадался на глаза.

2.

УЛОВКИ ДИЗАЙНА

Технологии используют дизайн, известный как «темный паттерн», основанный на человеческой психологии и провоцирующий вас подписаться, купить или поделиться очень личной информацией.

Типичные приемы – это использование определенных цветов, расположение кнопок, неясные тексты или неполная информация. Иногда эти уловки очевидны, однако чаще всего их сложно определить. Возможно, некоторые из них вы заметили при оформлении подписки на сервис или во время онлайн-покупок. Эти приемы повсюду именно потому, что они действенны: заставляют нас кликнуть, подписаться, чаще покупать и снова возвращаться на сайт. Чем лучше вы разбираетесь в ловушках и манипуляциях, заложенных в дизайн сайтов и приложений, тем более информированными и сообразительными становитесь.

Чтобы перехитрить свои приложения, вы можете провернуть несколько трюков.

Распознавайте, когда вами манипулируют: первое, что вы можете сделать – просто знать об использовании таких методов.

Сделайте снимок экрана и поделитесь: каждый раз, когда вы сталкиваетесь с манипулятивным дизайном в сети, делайте скриншоты и делитесь ими с друзьями (не раскрывайте персональных данных, ведь безопасность прежде всего!). Вы также можете обратиться к компаниям и попросить их не манипулировать.

Сохраняйте спокойствие: если вы видите на странице онлайн-магазина обратный отсчет времени, спросите себя: «Это действительно что-то срочное?». Если же вы поймали себя на том, что нажимаете кнопку без особого желания совершить покупку, обратите внимание на текст, кнопки или цвета сайта. Если вам не совсем ясна информация,

3.

СОХРАНЯЙТЕ МЕДИАГРАМОТНОСТЬ

Подобно тому, как вы можете обойти манипулятивные функции и дизайн сайтов, вы можете распознавать новости или сообщения, вводящие людей в заблуждение.

Вы, наверное, слышали о таких проблемах, как дезинформация и фейкньюз. Вы можете научиться распознавать дезинформацию, если будете анализировать критически все новости – особенно если они кажутся вам удивительными, возмутительными или звучат слишком хорошо, чтобы быть правдой.

В конце концов, вы захотите проверить правдивость сообщений, особенно если планируете поделиться ими с родными или друзьями.

На каком сайте опубликована новость?
Кто и когда ее написал?
О чем помимо заголовка сообщает вся статья?
На какие источники ссылается автор?

Lorem ipsum

Если вы считаете новость дезинформацией и хотите остановить ее распространение, сообщите об этом в службу поддержки, на большинстве сайтов такая есть. Также задумайтесь, стоит ли дальше быть подписанным на аккаунт, который публикует непроверенную информацию.

DATA DETOX KIT

DATA DETOX KIT

6 СПОСОБОВ КОНТРОЛИРОВАТЬ ДЕЗИНФОРМАЦИЮ В СЕТИ

Приложения, веб-сайты и онлайн-медиа незаменимы для доступа к новостям, лайфхакам и развлечениям. Однако среди всего этого контента может быть сложно найти именно то, что вам необходимо.

Более того, бывает трудно понять, правда это или вымысел, наткнувшись на видео, картинку или статью в интернете.

Персонализированные алгоритмы, которые пытаются вас профилировать, шокирующие заголовки, отредактированные фото или видео могут убедить вас в совершенно другой реальности. То, что вы видите онлайн, не всегда то, чем кажется.

В этой части «Цифровой детоксикации» мы расскажем вам о самых популярных дезинформационных темах и вирусных словах. Начнем с анализа вашей ответственности, после чего исследуем более широкую картину и дадим советы, как найти место среди виртуального вихря информации.

Поехали!

5. ПОИСК ПРАВДЫ В СЕТИ

Термин «фейкньюз» используется для обозначения широкого диапазона неточной или вводящей в заблуждение информации. Сюда также относятся сатира, плохо исследованный или непроверенный контент, мистификация и мошенничество. Фейковые новости не всегда распространяются злонамеренно, но независимо от причины публикации, результат обычно одинаковый: люди считают неправду правдой или верят в событие, которого на самом деле не было.

В лучшем случае фейковые новости подаются под видом юмористического мема. В худшем – это неточная медицинская или ложная политическая информация. Даже прилагая все усилия, исследуя источники и задавая правильные критические вопросы, вы можете остаться в замешательстве. Но знайте, что вы не одни!

Свистать всех наверх
Если сайт не признает своих ошибок, не значит, что он их не совершает. Фактически, самые надежные издания – осторожны с правдой, они нанимают сотрудников или целые отделы, которые занимаются исключительно проверкой фактов.

Ищите платформы, которые признаются ошибки и публикуют уточнения или исправления. Еще лучше, когда обновление резюмируется в самом верху статьи, а также публикуется в социальных сетях, и у вас нет необходимости долго и усердно искать.

6. ВЫБЕРИТЕСЬ ИЗ ИНФОРМАЦИОННОГ О ПУЗЫРЯ

После того как веб-сайты и приложения создадут профиль на основе ваших интересов и предпочтений, вы можете оказаться в искусственно образованном пузыре, когда вам подсовывают истории, подобные тем, на которые вы уже отреагировали. Как это ограничивает вас или изменяет поток информации?

Находясь в пузыре, люди могут видеть совершенно разные истории, заголовки новостей, статьи и рекламные объявления, как показано в интерактивной статье Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed).

Если вы понимаете, что просматриваете алгоритмически подобранный, разработанный специально для вас контент, возникает вопрос: как можно выбраться из этого пузыря?

Смените направление и разбавьте свои новости
Хороший способ выбраться из созданного для вас пузыря – подписаться на сервисы, которые собирают новости из разных источников и с различными точками зрения. RSS-каналы, различные рассылки, форумы, где представлен широкий спектр мнений, помогут вам увидеть происходящее за пределами пузыря. Можно начать с Global Voices (globalvoices.org) и Syllabus

datadetoxkit.org **#datadetox**

Проект создан
TACTICAL TECH

Партнеры проекта
Save the Children 100 ANNI
IFLA

Funded by the European Union

1.

ОСОЗНАЙТЕ СВОЕ ВЛИЯНИЕ

Лайки, обмены, ретвиты, репосты – все эти действия описывают ваш процесс взаимодействия с интернет-сообществом и то, как вы влияете на информационную среду. Когда с изображением, видео или публикацией взаимодействует большое количество людей, они быстро распространяются, становясь «вирусными».

Найдите минутку и задайте себе вопрос: «Каким образом я влияю на интернет?». Вспомните, когда в последний раз вы увидели шокирующую или смешную статью, заголовок, видео или изображение, и уже через несколько секунд отправили его друзьям? Исследования показывают: чаще всего вирусным становится тот контент, который вызывает у вас страх, отвращение, трепет, гнев или тревогу. Если это то, что вы сделали сегодня утром, не вините себя!

Делиться – значит заботиться
Обмен – это форма участия. Делясь чем-то в сети (это может быть что угодно), вы повышаете шансы на то, что этот контент станет вирусным. Хотите ли вы связывать свое имя с изображением или текстом, если оно, например, окажется фейком? Перед тем как делиться ссылкой, подумайте, может ли эта информация быть ложной, разрушительной или токсичной.

2.

ПОДУМАЙТЕ ДВАЖДЫ

Когда в последний раз вы проходили примерно такой тест:

- Какое вы десятилетие?
- Какое ваше тотемное животное?
- Какой ваш идеальный отпуск?
- ...этот список можно продолжить!

Несмотря на то, что такой тест может быть довольно веселым, не исключено, что вопросы были тщательно разработаны для сбора информации и классификации личности человека на основе так называемых психометрических данных.

Ответы во время прохождения теста «Какой ты персонаж Симпсонов?» вместе с другими вашими привычками могут отслеживаться в браузере, приложении или подключенными к сайту картами лояльности. Такая информация может дать аналитикам представление о том, какой вы человек, что вам небезразлично, как заставить вас купить пару обуви... Или даже создать портрет и повлиять на ваш голос на предстоящих выборах.

Больше секретов
Первое, что приходит на ум, когда вы думаете о частной информации – это ваши пароли, идентификационный код и номер банковской карты. Однако информация о ваших амбициях, страхах и раздражителях такая же личная, как и детали финансовой деятельности. Ее можно считать ценными данными для аналитиков, которые изучают ваши личностные характеристики. Прежде чем отвечать на вопросы тестов или участвовать в опросах, хорошо подумайте, хотите ли вы делиться секретами.

3.

НЕ ВЕДИТЕСЬ НА ПРИМАНКУ

Кликбейт (click bait) – это термин, используемый для описания сенсационного, неточного или вымышленного заголовка, предназначенного, чтобы люди нажали на него или перешли по ссылке. Чем больше внимания привлекает статья, видео или изображение, тем больше денег они могут принести. А это значит, что создатели будут идти на многое, чтобы заставить вас нажать на заголовок или поделиться контентом с другими пользователями.

На основе профиля личности, созданного используемой вами платформой (например, Facebook или Instagram), лента новостей подсовывает вам заголовки. Они создаются таким образом, чтобы задеть ваши эмоции, и тогда вы с большей вероятностью кликнете по ним.

Не всегда, но кликбейт может оказаться дезинформацией. Как только вы научитесь ее распознавать, заметите повсюду: на YouTube, в блогах и таблоидах.

Дойдите до первоисточника
Столкнувшись с кликбейтом, не останавливайтесь на заголовке. Если он похож на безопасную ссылку, перейдите на статью и узнайте, кто автор, когда текст был опубликован, на какие источники ссылается издание. Возможно, статься помечена как реклама или платный контент. Может быть, текст относится к категории «мнения». Такие детали помогут понять, стоит ли подобная информация вашего времени и энергии.

4.

БЕРЕГИТЕСЬ ПОДДЕЛОК

Дипфейки (deepfake) – это видео, аудиоклипы или изображения, на которых с помощью программы заменили чье-то лицо, движения или изменили слова. Хотя термин «дипфейк» появился относительно недавно, в той или иной форме они существуют целую вечность. Еще проще создать так называемые «чипфейки» – дешевые подделки, не требующие сложных технологий, но вводящие в заблуждение. Такой эффект создает ложная подпись к фото и видео или использование устаревшего контента для иллюстрации новых событий.

Может показаться, что по-настоящему бороться с фейками невозможно, но все-таки вы можете кое-что сделать – быть начеку.

Будьте начеку, исследуйте
Как и в случае с кликбейтами, не принимайте ничего за чистую монету. Если увиденное фото или видео кажется вам неправдоподобным и возмутительным, осознайте это чувство и подумайте, что может стоять за этой информацией. В противном случае, если вы заметите, что одно и то же изображение заполонило вашу ленту или несколько друзей прислали вам его, возможно, нужно поискать первоисточник.
Это именно тот случай, когда нужно задавать вопросы:

Кто его опубликовал (Какой сайт? Кто автор)? Когда это было опубликовано? Если это фото, выполните обратный поиск изображений с помощью TinEye (tineye.com) и посмотрите, где оно еще встречается.

Перепроверяйте другие источники новостей, прежде чем поверить им и поделиться с друзьями и близкими.