4.

ЗАХИСТІТЬ СВІЙ БРАУЗЕР

Ваш браузер - це ваш портал в Інтернет. Якщо ви підозрюєте, що він теж робить значний внесок у збір даних про вас, то маєте рацію.

Веб-браузери знають про вас дуже багато - де ви перебуваєте, що шукаєте, які веб-сайти відвідуєте - і можуть передавати цю інформацію в треті руки.

Рекомендуємо встановити кілька додаткових сервісів, відомих як "додатки й розширення" (це прості в установці міні-програми для вашого браузера, які можуть зробити перегляд сайтів більш приватним).

Щоб заблокувати рекламу, встановіть uBlock Origin: додаток для браузера, який не тільки блокує рекламу, але також є блокатором загального призначення.

Щоб переконатися, що ваше з'єднання з веб-сайтами максимально безпечне, встановіть HTTPS Everywhere: розширення для браузера, яке гарантує, що ваша взаємодія з багатьма основними веб-сайтами шифрується та захищається.

5.

ПЕРЕДАЙТЕ ДАЛІ

Долучилися в минулому до накопичення даних про своїх друзів, відмічаючи їх на фотографіях і в дописах?

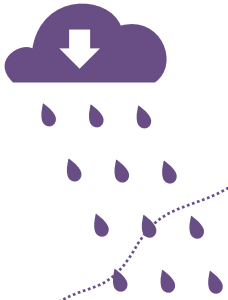
Полегшіть їм вантаж даних (і заодно заспокойте власну суспільну свідомість), знявши відмітки з максимальної кількості фотографій і дописів.

Передайте далі! Важливо заохочувати друзів, родичів і колег приєднатися до наших зусиль із контролю за даними, які від нас втікають. Якщо ми діятимемо спільно, то зможемо гарантувати кращий захист найвразливішим членам нашої спільноти.

створено
TACTICAL TECH

за підтримки
Firefox

datadetoxkit.org
#datadetox



DATA DETOX KIT

ПОДАРУЙТЕ ДАНИМ НА СМАРТФОНІ ГАРМОНІЮ

Для кращого захисту конфіденційності в мережі

Вас непокоїть реклама, яка слідкує за вами в Інтернеті? Вас турбує думка про те, що всі ваші дії онлайн відстежуються? Ви хочете захистити свої особисті дані, але не знаєте, з чого почати? Ми вам допоможемо!

Немає жодної потреби викидати смартфон і жити в печері. Легкі зміни в користуванні мобільним пристроєм допоможуть вам почуватися в Інтернеті безпечніше.

Вважайте описані тут кроки своєю базовою версією "Набору для детоксикації даних".

Якщо у вас є час лише на кілька справ, виконайте ці прості інструкції й відчуйте позитивні результати детоксикації вже зараз. А оскільки це лише базові кроки, за бажання ви можете знайти за посиланнями додаткові поради, які дозволять вам продовжити шлях до повністю збалансованого життя в Інтернеті. Уперед!

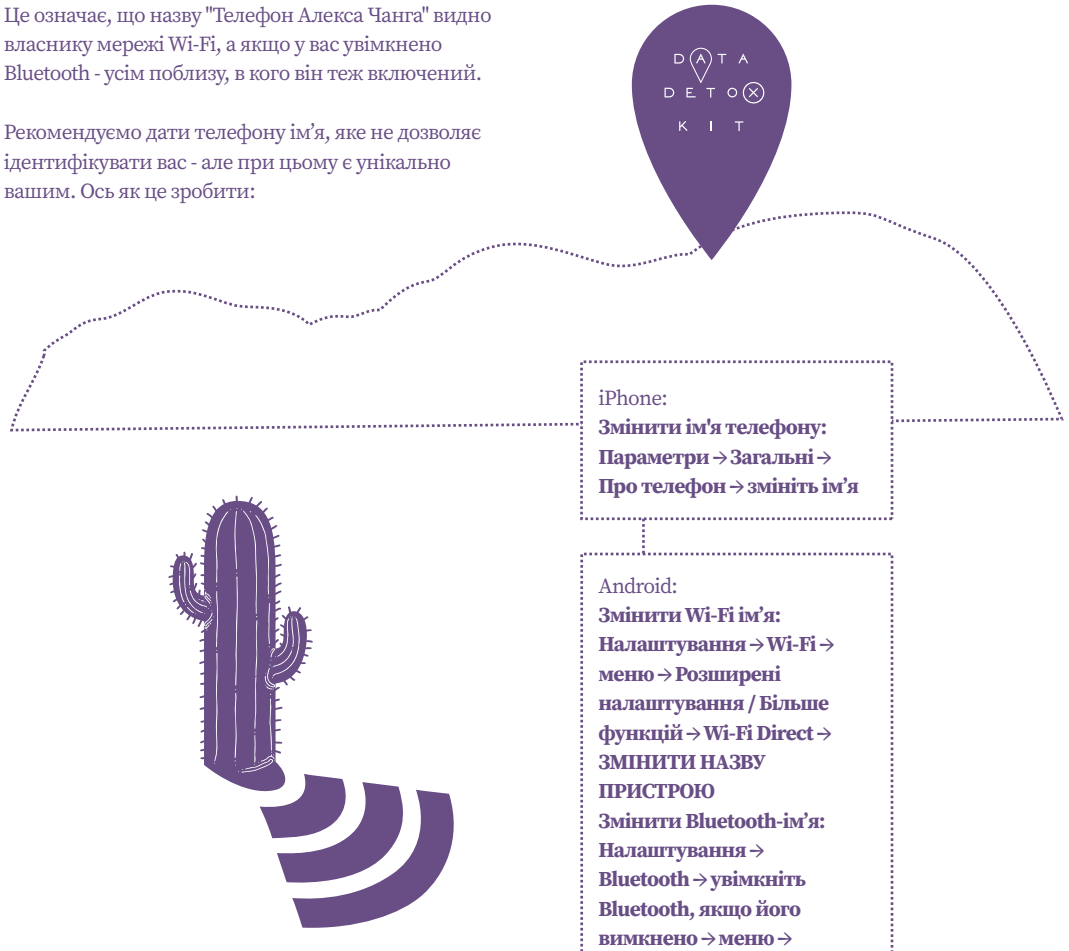
1.

НЕ НАЗИВАЙ МЕНЕ СВОЇМ ІМЕНЕМ

У якийсь момент, можливо, ви дали своєму телефону ім'я для під'єднання до Wi-Fi, Bluetooth чи обох типів мереж - або ім'я було автоматично створено під час налаштування телефону.

Це означає, що назву "Телефон Алекса Чанга" видно власнику мережі Wi-Fi, а якщо у вас увімкнено Bluetooth - усім поблизу, в кого він теж включений.

Рекомендуємо дати телефону ім'я, яке не дозволяє ідентифікувати вас - але при цьому є унікально вашим. Ось як це зробити:



iPhone:
Змінити ім'я телефону: Параметри → Загальні → Про телефон → змініть ім'я

Android:
Змінити Wi-Fi ім'я: Налаштування → Wi-Fi → меню → Розширені налаштування / Більше функцій → Wi-Fi Direct → ЗМІНИТИ НАЗВУ ПРИСТРОЮ
Змінити Bluetooth-ім'я: Налаштування → Bluetooth → увімкніть Bluetooth, якщо його вимкнено → меню → ЗМІНИТИ НАЗВУ ПРИСТРОЮ → вимкніть Bluetooth

2.

ЗІТРІТЬ СЛІДИ МІСЦЕЗНАХОДЖЕННЯ

Оскільки дані, що стосуються місцезнаходження, можуть так багато сказати про те, хто ви й що вас цікавить, за ними полюють великі IT-компанії та брокери даних: всі хочуть їх отримати. Може здатися, що це лише випадкові фрагменти інформації, проте в сукупності вони дозволяють сформувати цілісне уявлення про те, що ви за людина.

Вимкніть у телефоні служби геолокації, якщо не користуєтеся ними в даний момент. Це також дозволить батареї служити вам довше - бонус! Ви можете легко увімкнути геолокацію знову, коли вам, скажімо, знадобиться карта чи додаток для відстеження погоди.

3.

НАВЕДІТЬ ЛАД У ДОДАТКАХ

Можливо, ви не підозрювали, що додатки для соцмереж, ігри та додатки для визначення погоди цікавляться вашими даними... але вони здатні збирати досить велику кількість інформації.

Видалення додатків може бути потужним засобом детоксикації вашого цифрового життя.

Крім того, є шанси, що таке прибирання зменшить споживання трафіку й заряду акумулятора або збільшить загальну продуктивність (залежно від програми).

Android:
Налаштування → Безпека та місцезнаходження / Місцезнаходження → вимкніть встановлення місцезнаходження.

iPhone:
Параметри → Конфіденційність → Служби геолокації → вимкніть їх.

Android:
Налаштування → Програми → Виберіть додаток, який ви хочете видалити → Видалити.

iPhone:
Натискайте на один додаток, поки всі вони не почнуть тремтіти; у верхньому лівому куті кожного додатка з'явиться невеликий хрестик. Щоб видалити додаток, торкніться невеликого хрестика на його значку. Щоб повернутися до звичного вигляду, натисніть кнопку "Додому".

4.

ЗАХИСТІТЬ СВОЇ ВІРТУАЛЬНІ ЦІННОСТІ

Так само, як ви піклуєтеся про цінні речі в себе вдома, те саме слід робити з інформацією, яку ви зберігаєте віртуально. Не має значення, йдеться про фінансовий стан, скани паспорта чи навіть адресу й номер телефону, — варто подумати, де ви зберігаєте найбільш цінні особисті дані та як їх захистити.

Швидке очищення — хороший варіант маленького покращення за кавою. Знайдіть конкретну інформацію, яка зберігається у вас в електронній пошті, і видаліть її: наприклад, скани паспорта, банківські дані чи інформацію про страховку. Якщо вам це ще раз знадобиться, можна завантажити чи роздрукувати цю інформацію, а потім видалити з поштової скриньки.

Глибоке очищення більш ретельне, і ним корисно займатися раз на рік. Заархівуйте все на електронній пошті чи в соцмережі, завантажте все на комп'ютер та видаліть вміст з облікового запису, щоб почати з чистого аркуша.

Підказка: не просто видаляйте — також очистіть кошик і видаліть тимчасові файли!

Що робити з резервною копією, вирішуєте ви: її можна завантажити у хмару чи зберегти на зовнішній жорсткий диск або флешку. Не має значення, який варіант обирати — головне, щоб ви не втратили цю інформацію, вона була захищена надійним паролем, а вам було зручно користуватися цим способом.

5.

ПЕРЕДАЙТЕ ДАЛІ

Про це часто забувають, але мережа інтернет не просто так називається "мережею". Ми всі поєднані онлайн, не лише як "друзі" в соцмережах, але й через контакти в електронних листах та фото, якими ми ділимося. Коли ви налаштовуєте безпеку облікових засобів, підбираєте надійні паролі та чистите інформацію про себе онлайн, це приносить користь не лише вам — завдяки вашим зусиллям також покращується безпека інших.

Коли ви чистите електронну скриньку й акаунти в соцмережах, подумайте, що ще такого можна завантажити і видалити, що може допомогти вашим друзям чи колегам: банківську інформацію сестри, код доступу до офісу або скан синового паспорта — їх легко видалити, але вони можуть завдати чимало турбот, якщо потраплять до людини з поганими намірами.

Передайте далі! Кількох простих кроків достатньо, щоб покращити рівень онлайн-безпеки. Поділіться цією інструкцією для цифрового детоксу з друзями, рідними чи колегами, щоб і вони могли змінити свої цифрові звички так, як їм це зручно.

DATA DETOX KIT

SHIFT СВОЇ НАЛАШТУВАННЯ,*

щоб ваші дані були в безпеці

Якби інтернет потрібен був лише для того, щоб ділитися фоточками собак у костюмі динозавра, паролі були б не надто й потрібні.

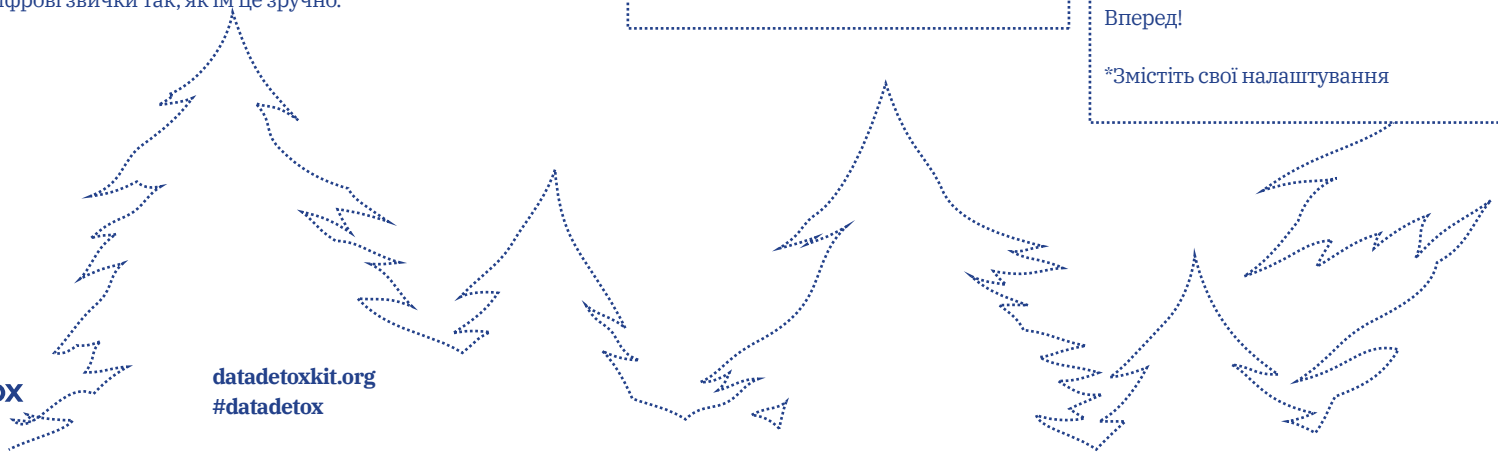
Але в інтернеті ви також сплачуєте рахунки, записуєтесь до лікаря, змінюєте виборчу адресу.

Подумайте про всі ваші "віртуальні цінності", які ви завантажуєте в інтернет — і зберігаєте на своїх пристроях — чому б не стежити за їхньою безпекою так само, як за гаманцем чи ключами?

В рамках Цифрового детоксу ви дізнаєтеся, що можна зробити, щоб покращити рівень своєї безпеки онлайн.

Вперед!

*Змістіть свої налаштування



створено
TACTICAL TECH

за підтримки
Firefox

datadetoxkit.org
#datadetox

1.

ЗАМКНІТЬ СВОЇ ЦИФРОВІ ДВЕРІ

Блокування екрану: пароль, графічний ключ, відбиток пальця чи ідентифікація за обличчям, які ви використовуєте, щоб розблокувати свій пристрій — один з найкращих способів захисту від людей, які хочуть без дозволу добратися до вашого телефона. Але блокування є різні, а вибрати між ними часом важко. Будь-який спосіб блокування телефона, планшета чи комп'ютера — краще, ніж взагалі жодного. Але так само, як бувають різні замки на двері, деякі способи блокування екрану надійніші за інші.

Найбільш надійний метод блокування — довгі унікальні паролі. Це означає, що ви розблоковуєте пристрій за допомогою пароля, який включає літери, цифри та спеціальні знаки.

Скажімо, ви зараз розблоковуєте телефон за допомогою свайпу. Ви можете відразу ж покращити рівень безпеки за допомогою довгого пароля. Чи може, ви використовуєте графічний ключ? Можливо, варто зробити його довшим? Чи у вас пін-код 1234? Спробуйте кинути гральні кубики сім разів і використати результат у якості піну.

2.

ВПУСТИ (ЛИШЕ) МЕНЕ

Створити якісний пароль просто. Потрібно лише дотримуватися кількох базових принципів. Ваші паролі мають бути:

Довгими: **паролі мають складатися принаймні з 8 знаків. А краще з 16-20.**

Унікальними: **кожен пароль, який ви використовуєте — на кожному сайті — має бути інакшим.**

Довільними: **паролі не мають бути логічними і їх не має бути легко вгадати. Для цього корисні менеджери паролів.**

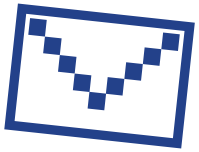
У найкращих паролях використовується поєднання літер, цифр та спеціальних знаків. Ця перевірена часом порада досі допомагає створювати більш надійні паролі, які важче зламати. На жаль, деякі системи не дозволяють використовувати спеціальні знаки (такі як @#$%-=+) у паролях, але довга комбінація літер і цифр все одно краща за коротку.

В ідеалі слід використовувати спеціальний менеджер паролів, щоб створювати і зберігати паролі. Менеджер паролів — наприклад, 1Password і KeePassXC, які рекомендують експерти з безпеки — це по суті додаток, який створений спеціально для того, щоб зберігати інформацію про ваші облікові записи та інші конфіденційні дані.

3.

ДОДАЙТЕ ДРУГИЙ КЛЮЧ

Налаштування двофакторної авторизації (2FA) чи багатофакторної авторизації (MFA) означає, що навіть якщо хтось і дізнається ваш пароль, ця людина, швидше за все, не матиме додаткового елемента, або фактора, який потрібен, щоб зайти в обліковий запис.



Подивіться на налаштування сайтів і додатків, якими ви користуєтеся найчастіше, щоб перевірити, чи можете ви налаштувати цей додатковий "ключ". Починайте з найважливіших додатків — тих, які пов'язані з фінансами, а також з електронної пошти, якою ви користуєтеся, щоб відновити доступ до інших облікових записів.

Google:
Залогіньтеся в myaccount.google.com → Безпека → 2-етапна перевірка → Почати

Facebook:
меню → Налаштування → Безпека та вхід → Двоетапна перевірка

Підказка: Коли ви налаштовуєте другий рівень перевірки, вам знадобиться додатковий спосіб підтвердити, що це ви. Намагайтеся уникати смс-ок в якості другого фактора, бо ви можете загубити телефон. Електронна пошта зазвичай надійніша.

4.

ЗРОБІТЬ ТАК, ЩОБ ВАС ПОЧУЛИ

Якщо вас не влаштовує переконливий дизайн чи дезінформація на сторінках, які ви читаєте, чи в додатках, які використовуєте, ви можете писати листи або твіти та повідомляти компанії, що ви не згодні з такими практиками. Коли компанії відчувають тиск з боку свого найціннішого капіталу — користувачів — є шанс, що вони будуть готові змінитися.

Якщо вам здається, що ваш зворотний зв'язок не чують, у вас є дуже впливовий інструмент: ви можете скористатися іншим сайтом чи додатком. Якщо ви повідомили, що вам не подобається щось із того, що робить сайт або додаток, а тоді ви перестанете заходити на сайт, а додаток видалите, і це зроблять достатньо людей — це помітять.

5.

ДІЛІТЬСЯ ІНФОРМАЦІЄЮ

Передайте далі! Про цю пораду легко забути, але вона має величезне значення. Розкажіть про те, що помічаєте, друзям, рідним і колегам — або навіть запропонуйте їм приєднатися до цифрового детоксу!

Всім непросто контролювати свої звички, пов'язані з телефоном. Важливо знайти підхід, який підходитиме вам і відповідатиме вашому стилю життя. Експериментуйте, поки не знайдете те, що працює саме для вас, і змінюйте свої звички відповідно до того, як змінюються й ваші потреби. Універсального рішення тут немає.

Будьте відкритими до нового і ставте запитання, щоб знайти саме таке збалансоване онлайн-життя, яке підійде особисто вам.

DATA DETOX KIT

ESCAPE ВІД НАЛАШТУВАНЬ ЗА ЗАМОВЧУВАННЯМ

щоб поліпшити своє цифрове благополуччя

Якщо ви постійно онлайн, ви не одні такі. Середньостатистична людина клікає, натискає та свайпає на телефоні понад 2600 разів щодня.

Хочете досягти більш здорової рівноваги між онлайн- та офлайн-життям? Про це і йдеться в цій частині "Детоксу даних".

Тут ви дізнаєтесь, як знайти вихід серед інформаційного шуму та що робити, щоб технології вам допомагали, а не шкодили. Немає "правильної" тривалості використання гаджетів на день. Починайте тоді, коли вам буде зручно, і рухайтеся далі.

Вперед!

*Втечіть від налаштувань за замовчуванням

створено
TACTICAL TECH

за підтримки
Firefox

datadetoxkit.org
#datadetox

1.

ПРОЖИВАЙТЕ МОМЕНТ

Ця порада складніша, ніж може здатися. Щоб навчитися проживати і відчувати момент, потрібна щоденна практика. Це як м'яз у мозку, який треба щодня тренувати, щоб він ставав сильнішим. Для початку можете звертати більше уваги на свої стосунки з технологіями, які ви використовуєте.

Якщо ваша мета — проводити менше часу в Фейсбуці, Інстаграмі чи в Снапчаті, змініть налаштування та дозволи цих додатків, щоб вони працювали так, як потрібно саме вам. У деяких додатках, таких як Інстаграм, навіть є функція, коли додаток турботливо нагадує, коли ви вже провели в ньому більше часу, ніж виділили на нього на сьогодні.

Інстаграм:
Профіль → меню → Налаштування → Обліковий запис → Ваша активність → Налаштувати щоденне нагадування

Якщо ви помітили, що телефон заважає розмовам у реальному житті, бо весь час дзвонить, вібрує чи мигтить, ви можете тимчасово поставити його на режим без звуку, покласти його екраном донизу чи навіть заховати його в кишеню чи сумку, щоб він не був перед очима.

2.

СПРОБУЙТЕ ПОМІТИТИ ТРЮКИ РОЗРОБНИКІВ

Переконливий дизайн, який також іноді називають "темними шаблонами", — це дизайн, що ґрунтується на психології людини та використовується, щоб спонукати вас на щось підписатися, щось купити чи поділитися більшою кількістю особистої інформації, ніж ви планували чи очікували.

Ви бачите ці фішки всюди саме тому, що вони ефективні: вони змушують нас частіше натискати, підписуватися, купувати та повертатися знову і знову. Що більше ви знатимете про приховані заклики та маніпуляції, вбудовані в сайти, якими ви користуєтесь, то більш підготовленими й поінформованими будете.

Ось що можна зробити, щоб перехитрити додатки.

Визначайте, коли вами маніпулюють: **Перше, що можна зробити — знати про використання цих технік.**

Робіть скріншоти і діліться: **щоразу, коли ви стикаєтесь із переконливим дизайном онлайн, зробіть скріншот і надішліть друзям (тільки приберіть всі особисті дані. Приватність — це головне!).**

Не панікуйте: **Якщо на сторінці онлайн-магазину є годинник зі зворотним відліком, запитайте себе: а це дійсно терміново? Якщо ви помічаєте, що натискаєте на кнопку навіть тоді, коли ви не мали такого наміру, подумайте, як сформульований текст на кнопках чи які кольори використовуються. Якщо вам щось незрозуміло, не поспішайте звинувачувати себе — подумайте, які формулювання використовуються на сайті чи в додатку, оскільки вони можуть бути нечіткими.**

3.

БУДЬТЕ ПОІНФОРМОВАНИМИ ПРО МЕДІА

Так само, як можна навчитися перехитрити ті функції та фішки дизайну, які мають змушувати вас скролити й натискати, можна також навчитися розпізнавати новини й пости, які написані так, щоб ввести вас в оману.

Швидше за все, ви вже чули про проблеми дезінформації та фейкових новин. Від дезінформації можна захиститися, якщо виробити звичку ставити критичні запитання до будь-яких новин, які ви споживаєте, особливо якщо ці новини здаються несподіваними, шокуючими чи неправдоподібно позитивними.

Загалом завжди потрібно перевіряти, правдива та чи інша новина чи оманлива — особливо, якщо ви плануєте поділитися нею з рідними чи друзями.

З якого сайту новина?
Хто (і коли) її написав?
Про що йдеться у статті загалом, а не лише в заголовку?
Про які джерела йдеться?

Якщо ви вирішили, що це дезінформація, і хочете, щоб вона не поширювалась далі, на більшості платформ є функція, де можна поскаржитися на запис. Ви можете також відписатися від сторінки, яка поширює такі новини.