4.

USUŃ ŚLADY

Przeglądarka w telefonie przechowuje wiele informacji na twój temat – gdzie się znajdujesz, co wyszukujesz, z jakich stron internetowych korzystasz – i może je przekazać dalej. Ale kilka zmian pomoże ci przejąć kontrolę.

Telefony, tablety i komputery mają zwykle fabrycznie zainstalowane przeglądarki, dla których twoja prywatność nie jest priorytetem. Zamiast nich możesz **pobrać i stosować przeglądarkę**, która **domyślnie chroni** twoją aktywność w sieci, zabezpieczając cię przed trackerami.

Jeszcze większą prywatność dadzą ci dodatki i rozszerzenia (łatwe do zainstalowania miniprogramy dla przeglądarki, które **zwiększają prywatność online**).

5.

ODTAGUJ SIEBIE I INNYCH

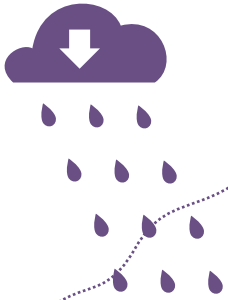
Zdarzyło ci się otagować zdjęcie i posty znajomych i dołożyć swoją cegiełkę do sterty zgromadzonych o nich danych?

Ulżyj im (i przy okazji swojemu sumieniu) i **odtaguj ich** z jak największej ilości zdjęć i postów.

Dziel się wiedzą! Zachęcaj znajomych, rodzinę i współpracowników do opanowania wymykających się spod kontroli danych. Jeśli wszyscy przyłożymy się do kontroli naszych cyfrowych śladów, pomożemy sobie nawzajem w detoksie.

Żeby zablokować szpiegujące cię reklamy i niewidzialne trackery, zainstaluj uBlock Origin (dla przeglądarek Chrome, Safari i Firefox) lub Privacy Badger (dla przeglądarek Chrome, Firefox i Opera).

Żeby zapewnić bezpieczne połączenie ze stronami internetowymi, o ile to możliwe, zainstaluj HTTPS Everywhere: rozszerzenie dla przeglądarki, które szyfruje i zabezpiecza twoje połączenie z wieloma popularnymi stronami internetowymi podczas przesyłu danych. Jeśli korzystasz z Safari, możesz ustawić domyślną wyszukiwarkę na produkt, który nie należy do firmy Google, na przykład DuckDuckGo, i będzie automatycznie przekierowywał cię na szyfrowane połączenia.



DATA DETOX KIT

KONTROLUJ DANE NA SMARTFONIE

i prywatność online

Mogłoby się wydawać, że twoje dane nie mówią o tobie nic wielkiego. W końcu kogo obchodzi, czy lubisz muzykę country, kupujesz za wiele par butów, czy planujesz wakacje z rocznym wyprzedzeniem?

Problem leży w tym, co się z twoimi danymi dzieje. Z czasem ze zgromadzonych na twój temat danych wyłaniają się prywatne informacje – o twoich nawykach, aktywności, relacjach, preferencjach, przekonaniach i tajemnicach. Stają się one widoczne dla tych, którzy je analizują i czerpią z nich korzyści, na przykład firm i brokerów danych.

Z Data Detox Kit dowiesz się, jak i dlaczego tak się dzieje. I poznasz praktyczne sposoby na kontrolowanie śladów swojej obecności w sieci.

Zaczynamy!

Autorzy
TACTICAL TECH

Wsparcie
Firefox

datadetoxkit.org
#datadetox

1.

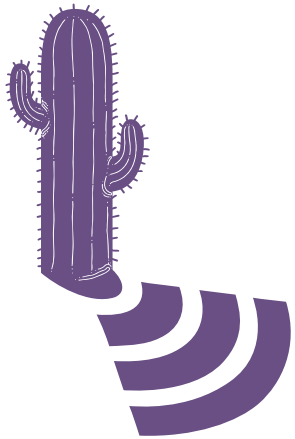
ZMIEŃ NAZWĘ URZĄDZENIA

W którymś momencie telefon otrzymał od ciebie „imię", które pojawia się, kiedy korzystasz z funkcji *Wi-Fi* i *Bluetooth*. Nazwa telefonu mogła również zostać automatycznie wygenerowana w trakcie konfiguracji. Oznacza to, że nazwa „Telefon Janka Nowaka" wyświetla się właścicielom sieci Wi-Fi oraz, jeśli masz włączony Bluetooth, wszystkim osobom, które również mają włączony Bluetooth i znajdują się w pobliżu.

Kiedy pojawiasz się w kawiarni, restauracji czy na lotnisku, nie anonsujesz się z imienia i nazwiska. I twój telefon też tego nie powinien robić.

Możesz **zmienić nazwę telefonu** na taką, która **nie wskazuje bezpośrednio na ciebie**, ale wciąż pozostaje osobista. Jak to zrobić?

iPhone:
Zmień nazwę telefonu:
Ustawienia →
Ogólne →
To urządzenie →
Zmień nazwę



Android:
Zmień nazwę dla funkcji Wi-Fi Ustawienia →
Wi-Fi →
Menu →
Zaawansowane / Więcej opcji →Wi-Fi Direct →
Edytuj nazwę telefonu
Zmień nazwę dla funkcji Bluetooth:
Ustawienia →
Bluetooth →
Włącz Bluetooth, jeśli jest wyłączony →
Menu →
Edytuj nazwę telefonu
Wyłącz Bluetooth

2.

ZNIKNIJ Z MAPY

Dane o lokalizacji to na pozór *przypadkowe strzępki* informacji, ale gdy spojrzy się na nie całościowo, mogą wyjawić coś **ważnego o tobie** i twoich zwyczajach, na przykład to, gdzie mieszkasz, gdzie pracujesz i gdzie lubisz spotykać się ze znajomymi. Dlatego tak wiele firm i brokerów danych chce je pozyskać.

To całkiem zrozumiałe, że apka do nawigacji ma dostęp do twojego położenia. Ale zaskoczyć cię może, jak wiele innych aplikacji dostało od ciebie zgodę na dostęp do danych o lokalizacji.

Przejrzyj zgody na dostęp dla każdej aplikacji i wyłącz usługi lokalizacji w tych, które ich nie potrzebują (czy gra naprawdę musi wiedzieć, gdzie jesteś?), i tych, którym nie chcesz zdradzać swojego położenia.

3.

POSPRZĄTAJ W APKACH

Apki do mediów społecznościowych, gier czy pogody są zainteresowane twoimi danymi. I mogą zebrać ich sporo.

Pozbywając się apek, z których nie korzystasz, zafundujesz sobie porządny cyfrowy detoks.

Poza tym takie porządki *zwalniają miejsce* w telefonie, zmniejszają zużycie danych i *zwiększają wydajność baterii*. A w zależności od usuniętej aplikacji poprawić się może również wydajność całego urządzenia.

Android:
Ustawienia →Aplikacje→
Ustaw dostęp do lokalizacji dla poszczególnych aplikacji

iPhone:
Ustawienia →Prywatność →
Usługi lokalizacji →
Ustaw dostęp do lokalizacji dla poszczególnych aplikacji

Android:
Ustawienia → Aplikacje →
Wybierz apkę, którą chcesz usunąć
Odinstaluj

iPhone:
Naciśnij i przytrzymaj ikonę apki do momentu, w którym pojawi się menu.

Wybierz opcję usunięcia aplikacji z listy.

Potwierdź usunięcie apki.