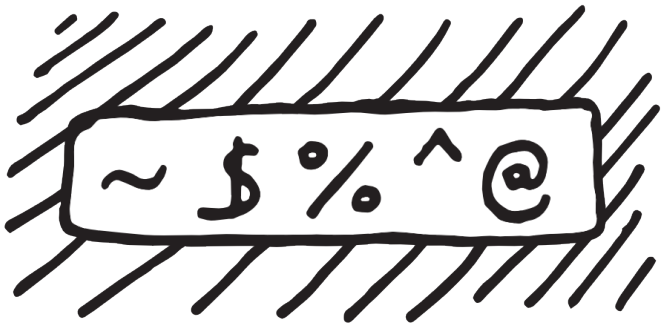
FUNDACJA PANOPTYKON

# PODSTAWY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI W SIECI

Rozwój technologii ma swoją cenę: dzisiaj na każdym kroku jesteśmy obserwowani przez kamery, śledzeni w sieci, a nasze dane są zbierane przez państwo i firmy, które na tym zarabiają. Fundacja Panoptykon jest jedyną organizacją w Polsce, która odpowiada na związane z tym zagrożenia i udowadnia, że nie jesteśmy wobec nich bezradni: nagłaśnia nadużycia; uczy, jak zabezpieczyć swoje dane, komputer, portfel czy telefon przed wykorzystaniem; walczy o to, by tworzone prawo chroniło naszą wolność i prywatność. Po prostu: kontroluje kontrolujących.

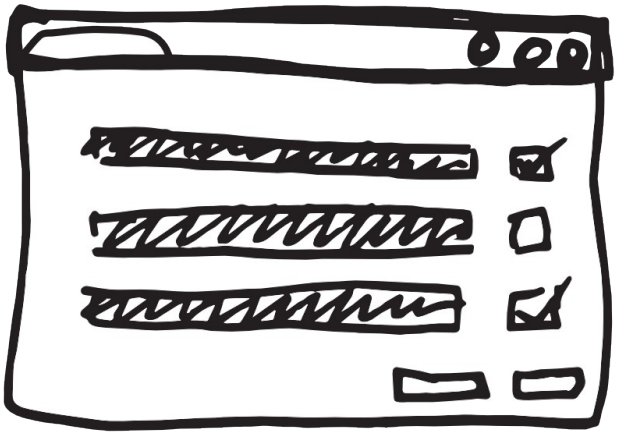
panoptykon.org



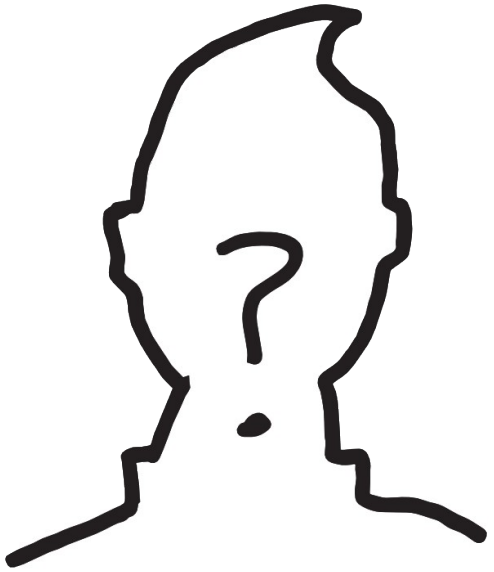

- Czy moje hasło do poczty zawiera w sobie słowa występujące w słowniku, a może informacje o mnie, np. datę urodzenia?
- Czy mam takie same hasła do wielu serwisów?
- Czy wiem, jak zabezpieczone są dane, które umieszczam w sieci, np. na wirtualnym dysku?


W 2014 roku doszło do kilkudziesięciu znaczących wycieków danych i ataków na firmy i serwisy WWW. W wielu z nich ogromną rolę odegrały słabe zabezpieczenia użytkowników i brak świadomości, jakie dane przechowują w sieci.

- Czy wiem, jak działa moja przeglądarka? Jakie dane (np. hasła) zapisuje?
- Czy zmieniłem(-am) kiedyś jej ustawienia bezpieczeństwa?
- Czy wiem, jakie informacje o mnie przesyłane są stronom WWW, które odwiedzam?




panopticlick.eff.org – test oceniający unikalność Twojej przeglądarki



- Czy przeczytałem(-am) regulamin serwisu społecznościowego, zanim założyłem(-am) tam konto?
- Czy wiem, co się dzieje z danymi, które mu udostępniam i które on zbiera o mnie (np. kiedy odwiedzam połączone z nim strony)?

# NIEDYSKRETNY PROFIL

## CZYLI CO WIE O TOBIE FACEBOOK (I INNE PORTALE SPOŁECZNOŚCIOWE)

## Jakie informacje zbiera?

Dane podawane przy tworzeniu konta i aktualizacji profilu

Udostępniane zdjęcia, filmy, statusy (nawet te nieopublikowane)

Profile, statusy i zdjęcia, które „lubisz”

Treść wysyłanych i odbieranych wiadomości

Informacje o „znajomych” i dane z książki adresowej

Informacje zbierane przez aplikacje mobilne

To, jakie strony odwiedzasz i co na nich robisz

Dane, jak często, jak długo i za pomocą jakich urządzeń korzystasz z portalu

Dane profilowe ułatwiają nie tylko wyszukanie Cię przez znajomych, ale też profilowanie przez portal i firmy reklamowe.

Nawet treści udostępnione tylko znajomym mogą być przekazane dalej. Facebook może użyć Twoich zdjęć np. do polecania produktów.

Na podstawie „lajków” można określić np. Twoją orientację seksualną czy wyznanie, nawet gdy ich nie ujawniasz.

Facebook nie szyfruje czatu na swoich serwerach, dlatego przesyłane treści nie są dobrze zabezpieczone przed wyciekiem.

Facebook zbiera informacje nawet o osobach, które nie założyły konta na portalu – tworzy im profile-cienie.

Korzystanie ze smartfona pozwala portalom zbierać dodatkowe informacje i zlokalizować Cię.

Historia odwiedzanych stron mówi o Tobie bardzo dużo, również to, czego świadomie nie chcesz ujawniać.

Nawet tak techniczne informacje pozwalają odróżnić Cię od innych i analizować Twoje rutyny.

Jeśli decydujesz się na korzystanie z portalu społecznościowego, podawaj tylko dane niezbędne do utworzenia konta.

Nie masz kontroli nad tym, co z informacją o Tobie zrobią inni. Zadbaj o ustawienia prywatności i nie udostępniaj treści, które chcesz chronić.

Każda strategia „lajkowania” mówi coś o Tobie. Zamiast śledzenia na Facebooku, korzystaj z newsletterów i kanałów RSS.

## Jak możesz się chronić?

Szyfruj Facebookowy czat za pomocą wtyczki Crypto.cat bądź programu Pidgin + OTR lub wybieraj inne kanały komunikacji.

Dawaj dobry przykład: nie udostępniaj listy kontaktów, nie publikuj informacji o innych osobach bez ich zgody.

Nie korzystaj z portali społecznościowych przez aplikacje, tylko za pomocą przeglądarek.

Blokuj śledzenie na stronach z przyciskami społecznościowymi (np. Disconnect). Nie loguj się przez konta społecznościowe do innych usług.

Nie masz na to wpływu. Możesz tylko zrezygnować z korzystania z portali społecznościowych.

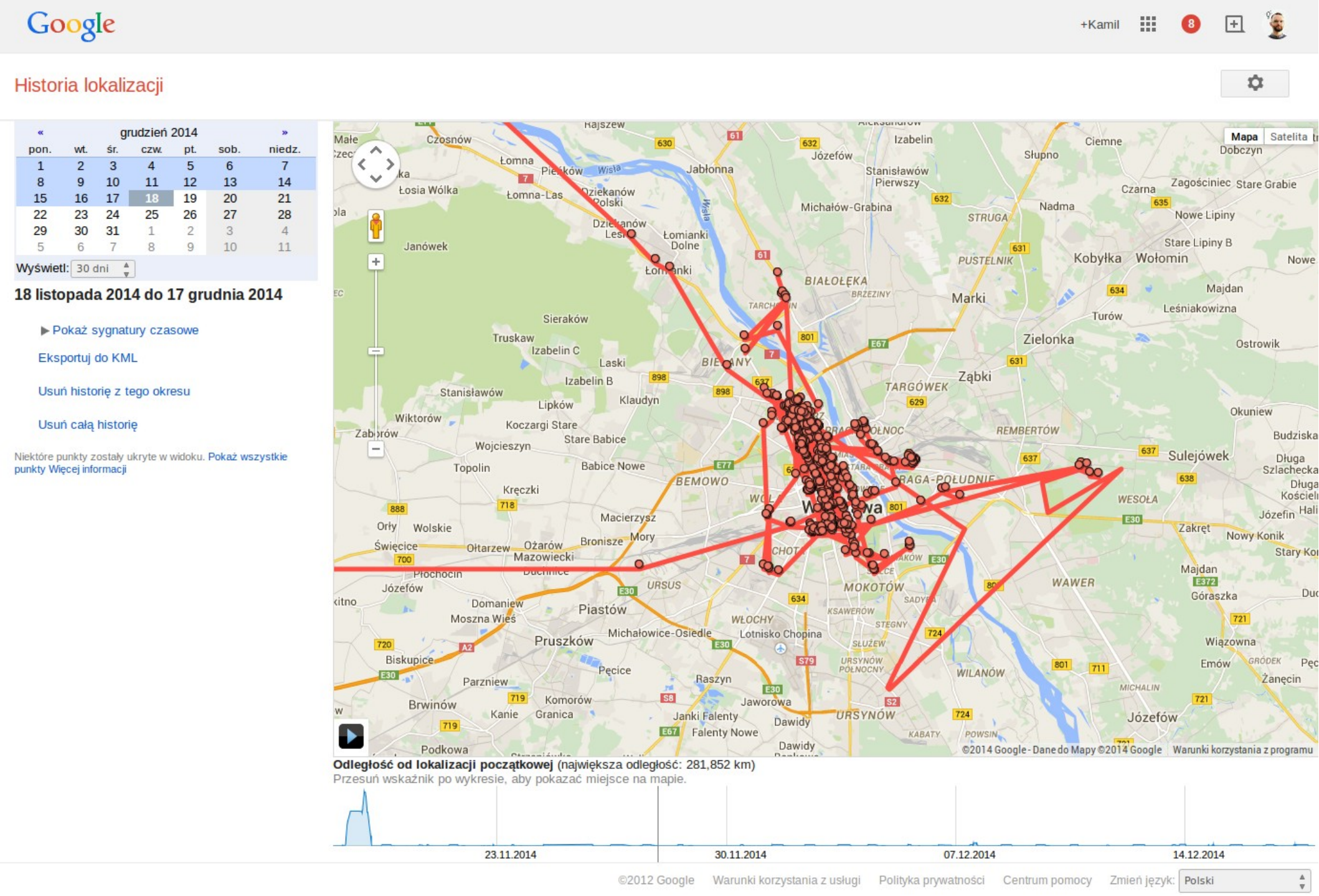
## Jakie to ma konsekwencje?

**Na podstawie danych z wielu źródeł można dowiedzieć się o Tobie o wiele więcej niż to, co samodzielnie udostępniasz. Na bazie tego algorytm decyduje np. o tym, jakie informacje i reklamy zostaną Ci wyświetlone. Przedstawiany w nich obraz świata może być wypaczony, a Ty – zamknięty w „bańce filtrującej”.**

**Świadomie podejmij decyzję, czy chcesz korzystać z portali społecznościowych. Nie ograniczaj do nich swojej obecności w Internecie – zaglądaj w różne miejsca i czerp informacje z wielu źródeł.**

AKADEMIA CYFROWA WYPRAWKA
cyfrowa-wyprawka.org
FUNDACJA PANOPTYKON
panoptykon.org
Ministerstwo Administracji i Cyfryzacji
Infografika powstała w ramach projektu „Cyfrowa Wyprawka dla dorosłych 2” współfinansowanego przez Ministerstwo Administracji i Cyfryzacji oraz indywidualnych darczyńców Fundacji Panoptykon

- Co wiedzą aplikacje, które ostatnio instalowałem (-am) na swoim smartfonie?
- Gdzie zapisywane są zdjęcia, które robię telefonem?
- Kto wie, gdzie jestem, gdy mam ze sobą komórkę?

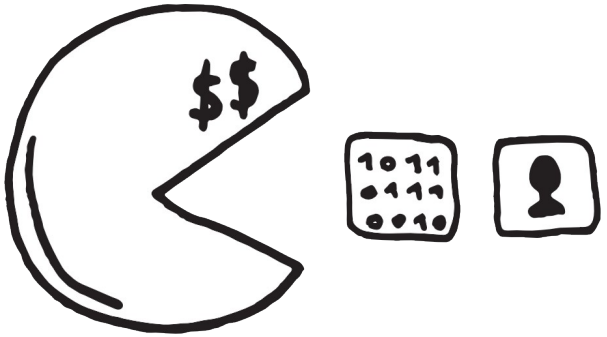



Google location history – widok historii lokalizacji telefonu z Androidem z włączonym Wi-Fi. Google zbiera informacje o każdej lokalizacji, w której telefon jest w zasięgu dowolnej sieci Wi-Fi.

# Do czego (i komu) mogą posłużyć dane?

Im więcej swoich danych zostawiasz w sieci, tym łatwiej atakować Cię **sprofilowanymi reklamami**, którym coraz trudniej się oprzeć i które stają się coraz trudniejsze do rozpoznania (odróżnienia od innych przekazów).


Skala zbieranych danych i sposób, w jaki wykorzystują je serwisy WWW, zwłaszcza sklepy i wyszukiwarki internetowe, do zaspokajania naszych potrzeb, wywołuje efekt tzw. **bańki informacyjnej** – ograniczania przekazu do informacji, które utwierdzają nas w naszych poglądach i przyzwyczajeniach.




Nasze **dane są towarem**, którym handlują nie tylko **złodzieje tożsamości**, ale i same serwisy internetowe.

Więcej danych w sieci to też łatwiejsze zadanie dla złodziei czy stalkerów albo wścibskich służb (jak amerykańska NSA).

# Jak odzyskać kontrolę?

- Skuteczna ochrona to nie oprogramowanie czy jednorazowa zmiana ustawień – to proces, który wymaga pewnych poświęceń.
- W sieci zawsze kieruj się zasadą ograniczonego zaufania i ćwicz swoją asertywność.
- Czytaj regulaminy, komunikaty itp. – możesz tam znaleźć wiele ważnych informacji.
- Nie udostępniaj nikomu swoich haseł i zadbaj o ich siłę, unikalność
  i odpowiednie zabezpieczenie.
- Unikaj usług ułatwiających Ci życie kosztem udostępniania Twoich danych, szczególnie tych, które zastrzegają sobie możliwość wykorzystania komercyjnego i handlu danymi. Rozważ alternatywne rozwiązania, szanujące Twoją prywatność.

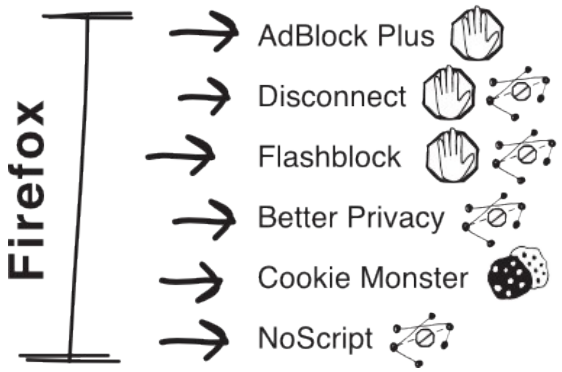
# Hasła – zasady BHP

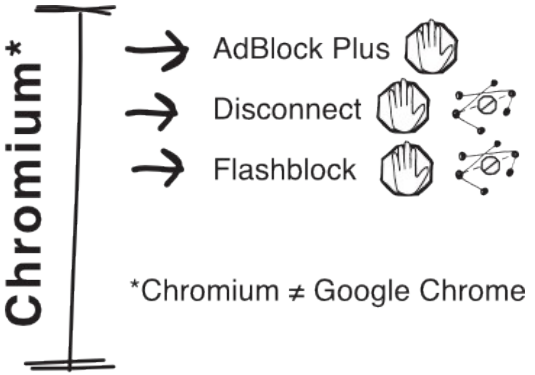
- Nigdy nie używaj swojego imienia, identyfikatorów ani nicków jako hasła (nawet ze zmianą wielkości liter, pisane wspak itp.).
- Nie używaj w haśle swojego imienia i nazwiska ani związanych z Tobą informacji, np. daty urodzin, nr PESEL itp.
- Nie używaj samych cyfr ani prostych pojedynczych słów.
- Używaj wielkich liter, znaków specjalnych (.,*#@!^& etc.) i cyfr (najlepiej równocześnie).
- Pamiętaj o zmianie hasła co pewien czas.
- Nie ignoruj informacji o wyciekach danych z serwisów, z których korzystasz. W razie wątpliwości zmień hasło.

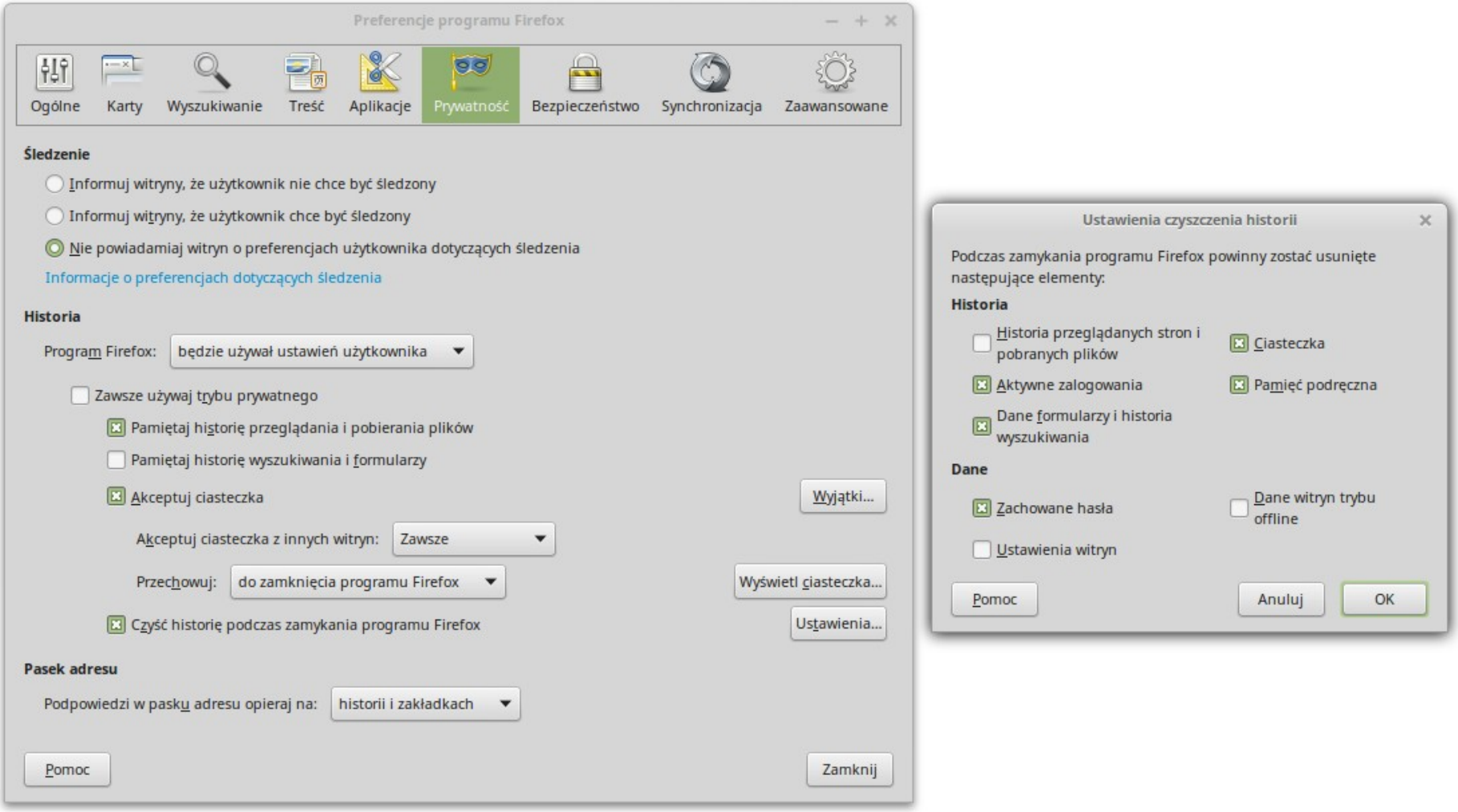
# Przeglądanie stron internetowych

- Wybierz bezpieczną przeglądarkę i zadbaj o ustawienia chroniące Twoją prywatność (np. włącz kasowanie ciasteczek podczas zamykania programu).

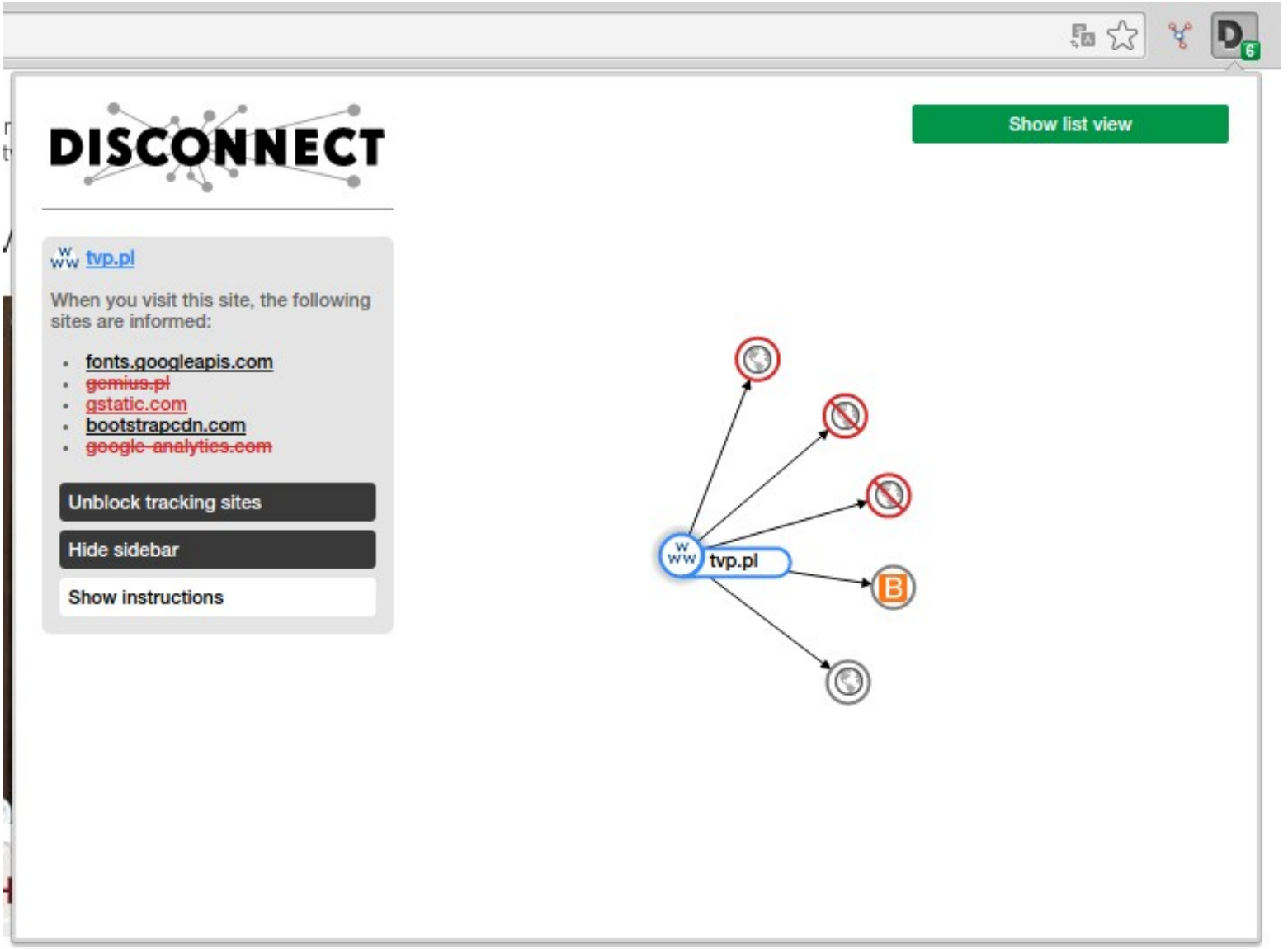
- Zainstaluj wtyczki, które:
  - blokują reklamy;
  - Chronią przed śledzeniem Twojej aktywności w sieci;
  - Pomagają zarządzać ciasteczkami.






Przykładowe ustawienia prywatności w przeglądarce Mozilla Firefox



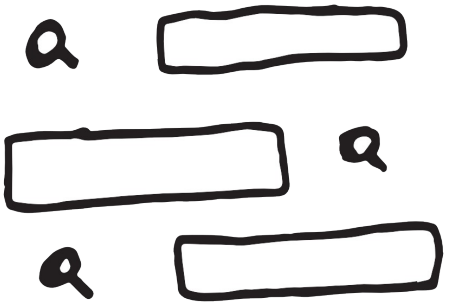

Wtyczka Disconnect i widok zablokowanych 4 z 6 stron śledzących ruch na stronie tvp.pl

# Poszukiwanie informacji w internecie

- Używaj wyszukiwarki, która nie zbiera informacji o Tobie i nie buduje na ich bazie profilu dla reklamodawców

→ DuckDuckgo.com

→ StartPage.com



# Rozmowy przez interenet

Korzystaj z komunikatorów, które szyfrują treść czatów (nawet tych prowadzonych przez Facebooka i Google Hangouts.

- → Adium + wtyczka OTR (Mac OS)
- → Pidgin + wtyczka OTR (Windows i Linux)
- → Jitsi (wszystkie systemy operacyjne
- → Xabber (Android)
- → ChatSecure (Android i iOS)


Porównanie popularnych komunikatorów pod kątem ich zabezpieczeń i szyfrowania

**https://www.eff.org/secure-messaging-scorecard**

# Korzystanie z poczty elektronicznej

- Korzystaj z usług dostawcy, który nie czyta Twoich e-maili.

Korzystaj z klienta pocztowego i szyfruj swoje e-maile.

→ Mozilla Thunderbird + wtyczka GPG (wszystkie Systemy operacyjne)

→ Mail + GPG Tools (Mac OS)

Porównanie popularnych komunikatorów pod kątem ich zabezpieczeń i szyfrowania

**https://emailselfdefense.fsf.org/**

# Dowiedz się więcej

- Cyfrowa Wyprawka (dla dorosłych)
  http://pnpt.org/cyfrowa
- Security in a box
  https://securityinabox.org/
- Electronic Frontier Foundation:
  https://www.eff.org/

FUNDACJA PANOPTYKON

# Wesprzyj Fundację Panoptykon!

pnpt.org/wspieraj



Prezentacja powstała w ramach projektu „Cyfrowa Wyprawka dla dorosłych 2” współfinansowanego przez Ministerstwo Administracji i Cyfryzacji oraz indywidualnych darczyńców Fundacji Panoptykon.

panoptykon.org