Aurea

@AureaLibe

[Poradnik] Jak uniknąć kontroli czatu i monitorowania prywatnych wiadomości

Parlament Europejski przyjął kontrolę czatów. Skanowanie naszych prywatnych wiadomości jest teraz dozwolone w Unii Europejskiej w imię „ochrony dzieci". Większość posłów do PE zagłosowała przeciwko tekstowi, ale ze względu na przepisy proceduralne do jego odrzucenia wymagana byłaby bezwzględna większość głosów. Nie udało się tego osiągnąć. Masowy nadzór został wyeliminowany. Od początku mojej kariery broniłem trzech prostych rzeczy: ludzi, wolności i prywatności.

Oto poradnik, jak działać. Ten artykuł to skrócona wersja mojego pełnego poradnika. Pełną wersję znajdziesz na dedykowanej stronie internetowej: exitchatcontrol.org

Dam ci wszystkie narzędzia do podjęcia działania, w postaci konkretnych kroków, ułożonych w kolejności od najprostszych do najbardziej zaawansowanych.

Najbardziej niebezpieczna wersja Chat Control opiera się na „skanowaniu po stronie klienta": oprogramowaniu, które odczytuje wiadomości bezpośrednio na telefonie, zanim zostaną zaszyfrowane.

W związku z tym sama sieć VPN lub proste szyfrowanie nie wystarczą, aby zapewnić ochronę. Każda z poniższych metod zapewni ci odrobinę większą ochronę. Nie musisz robić wszystkiego naraz. Ale opór zaczyna się od indywidualnych działań, a indywidualna odpowiedzialność zaczyna się od edukacji, a ja ci w tym pomogę.

Prawdziwą ochronę zapewni Ci przejście na darmowe oprogramowanie, które odrzuca to oprogramowanie szpiegujące. Dzięki temu odzyskasz kontrolę nad swoim urządzeniem, a co za tym idzie, będziesz mieć pełną kontrolę nad narzędziami, z których korzystasz.

Krok 1: Zmień dostawcę poczty e-mail (najpilniejsze działanie)

To pierwsza rzecz, którą powinieneś zrobić i która zapewni Ci najszybszą ochronę. Zamknij WhatsApp, Messengera i Telegrama i zainstaluj Signal.

To usługa przesyłania wiadomości równie prosta w obsłudze co WhatsApp, ale domyślnie szyfrowana metodą end-to-end, obsługiwana przez fundację non-profit, której zespół obiecał opuścić Europę, zamiast instalować skanowanie wiadomości.
Idź do signal.org
Zainstaluj aplikację, potwierdź swój numer, a następnie w Ustawieniach > Prywatność utwórz nazwę użytkownika, aby ukryć swój numer.
Jeśli chcesz pójść dalej, SimpleX Chat (simplex.chat) nie prosi o numer, adres e-mail ani żaden inny identyfikator. Nikt, nawet serwery, nie wie, kto z kim rozmawia. Mogę również polecić, podobnie, Session (getession.org). Najważniejsze: zachęć swoje kontakty do zainstalowania Signala. Szyfrowane wiadomości są bezużyteczne, jeśli tylko Ty z nich korzystasz. *Aby dowiedzieć się więcej, zapoznaj się z pełnym przewodnikiem dostępny tutaj.*

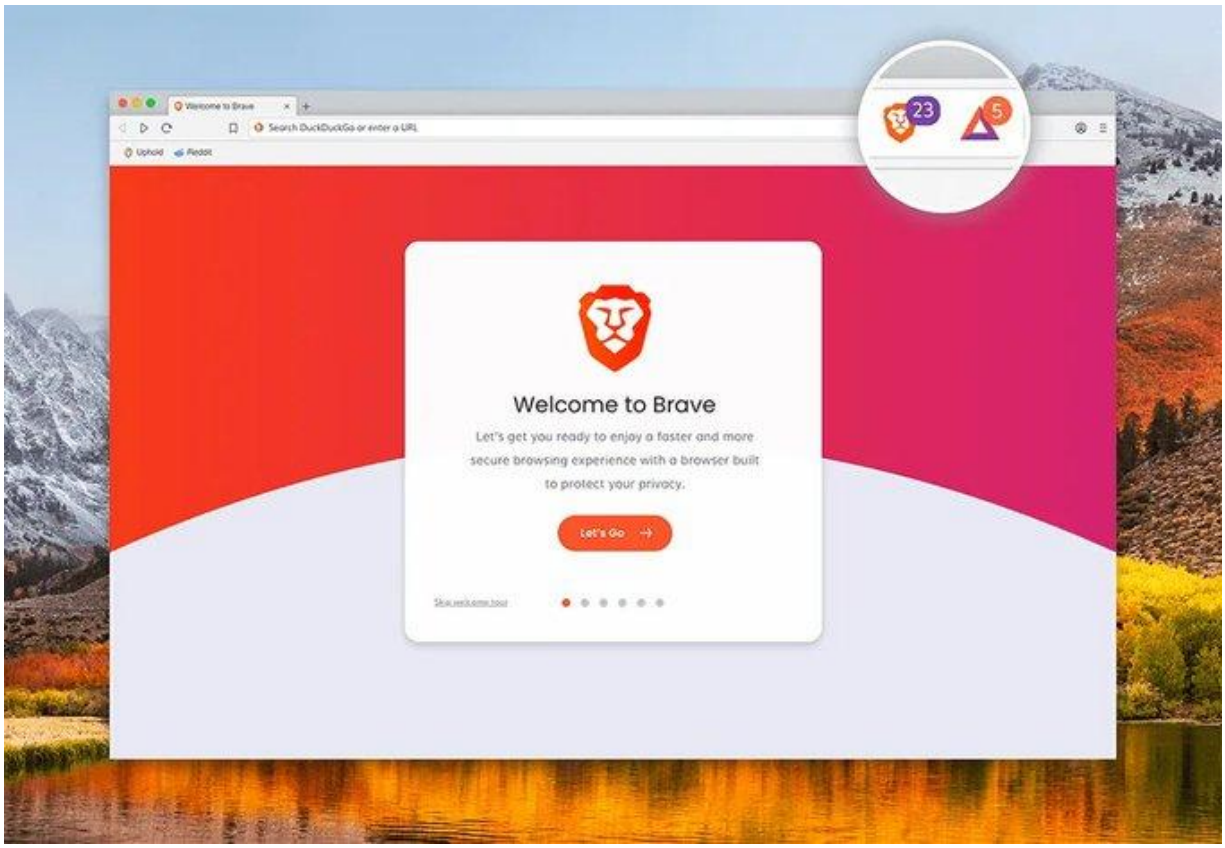
Krok 2: Zamknij Gmaila

Gmail odczytuje Twoje wiadomości e-mail i działa w Stanach Zjednoczonych, pod ich jurysdykcją. Opuszczenie go to ogromna korzyść przy minimalnym wysiłku. Załóż konto w Proton Mail (proton.me), z siedzibą w Szwajcarii i szyfrowaną. Darmowy plan to wszystko, czego potrzebujesz, aby zacząć. Po rejestracji skorzystaj z narzędzia „Easy Switch", aby zaimportować stare wiadomości i kontakty, skonfigurować przekierowanie z Gmaila i powiadomić kontakty o nowym adresie.

Równie solidną alternatywą, którą polecam, jest Tuta (tuta.com), niemiecki, całkowicie darmowy.
Aby dowiedzieć się więcej, zapoznaj się z pełnym przewodnikiem dostępny tutaj.

Krok 3: Zmień przeglądarkę, wyszukiwarkę i zrezygnuj z Google

Chrome szpieguje reklamy, a Google rejestruje każde Twoje wyszukiwanie. Zastępujemy oba. Aby bezboleśnie zmienić system, zainstaluj Brave (brave.com), przeglądarka internetowa
@BrendanEich
Pracował nad pierwszą przeglądarką internetową, wynalazł JavaScript, język powszechnie używany w Internecie, i był współzałożycielem przeglądarki Mozilla Firefox.



Brave jest jak Chrome, ale bez oprogramowania szpiegującego. Domyślnie blokuje reklamy i moduły śledzące, blokuje reklamy w YouTube, a nawet umożliwia dostęp do Tora jednym kliknięciem. To przeglądarka nastawiona na prywatność, która ochroni Twoje dane przed szpiegowaniem przez Google.
Jako darmową alternatywę mogę polecić Librewolf (librewolf.net) Nie polecałbym jednak przeglądarki Firefox, której twórca wygłosił kilka stwierdzeń sprzecznych z ochroną prywatności. Na koniec zmień domyślną wyszukiwarkę w przeglądarce, niezależnie od tego, czy używasz jej na komputerze, czy smartfonie. Polecam skorzystanie z wyszukiwarki Brave, Brave Search (search.brave.com) i jako alternatywę DuckDuckGo (duckduckgo.com).
Aby dowiedzieć się więcej, zapoznaj się z pełnym przewodnikiem dostępny tutaj
.

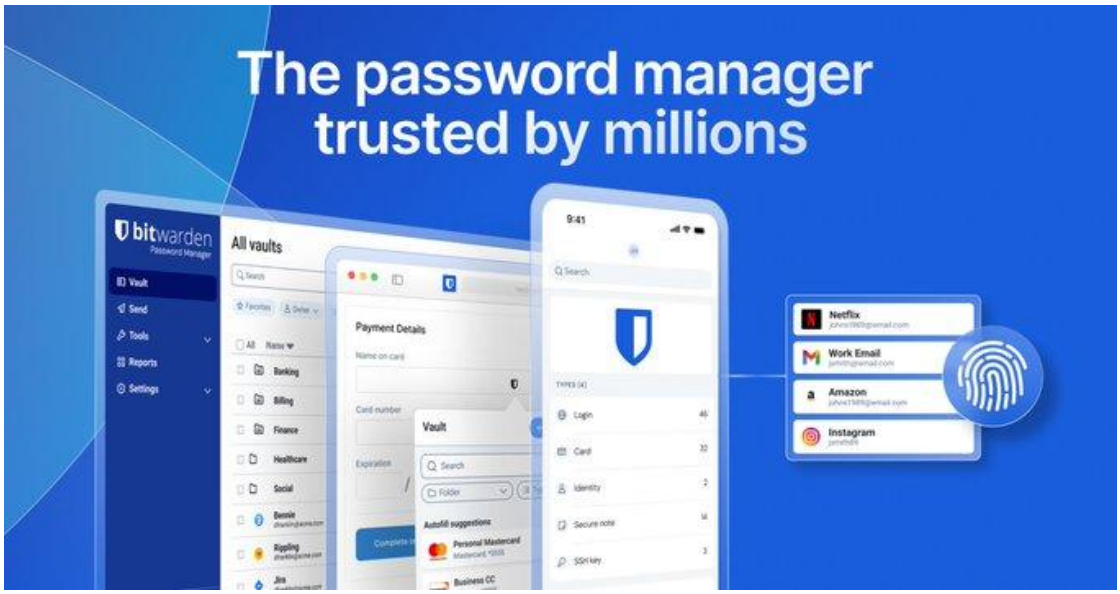
Krok 4: Użyj VPN

VPN nie chroni przed skanowaniem urządzenia, ale maskuje Twój adres IP przed dostawcą internetu i umożliwia dostęp do stron wymagających podania identyfikatora. Będzie to niezbędne, gdy anonimowość stanie się przeszłością.
Polecam **Mullvada** (mullvad.net): brak adresu e-mail, brak imienia i nazwiska, tylko numer konta, audytowana polityka braku logów i stała cena.

Konkretnie rzecz ujmując: 1. Przejdź do mullvad.net
(Jeśli strona jest dla Ciebie zablokowana, otwórz ją za pomocą przeglądarki Tor lub jej adresu .onion).
2. Kliknij „Wygeneruj numer konta". **Zapisz ten numer** w menedżerze haseł i nigdy go nie udostępniaj: to Twój jedyny klucz.
3. Zapłać. Jeśli Twoja karta bankowa działa, zachowaj prostotę. Jeśli zależy Ci na pełnej anonimowości, zapłać kryptowalutą: kliknij „Utwórz jednorazowy adres płatności" i prześlij kwotę z portfela. Monero zapewnia największą prywatność. Szczegółowy poradnik zakupu (Bitcoin, Monero przez swap) znajdziesz w tym kompleksowym przewodniku: https://x.com/AureaLibe/status/2016126634235953211
.
4. Pobierz aplikację na mullvad.net/pobierz
Wprowadź swój numer i połącz się z serwerem spoza Unii Europejskiej. Aktywuj „wyłącznik awaryjny".
Aby dowiedzieć się więcej, zapoznaj się z pełnym przewodnikiem dostępny tutaj.

Krok 5: Zabezpiecz swoje konta

Podstawą wszelkiego bezpieczeństwa jest unikalne i silne hasło dla każdej usługi.
Zainstaluj Bitwarden (bitwarden.com), darmowe i otwarte oprogramowanie. Utwórz długie hasło główne (frazę), zainstaluj rozszerzenie i aplikację, a następnie zapisz i zastąp stare hasła.



Ważne jest, aby przechowywać hasła w oprogramowaniu open source i nie powierzać ich Google ani Apple. Hasła dają dostęp do całego Twojego życia. Tak jak nie dałbyś kluczy do domu obcym osobom, tak samo Twoim obowiązkiem jest zrobić to samo ze swoimi hasłami.
Ponadto menedżer haseł umożliwia korzystanie z innego hasła na każdej stronie, co zwiększa Twoją prywatność i ogranicza ryzyko włamania.
Następnie **włącz** uwierzytelnianie dwuskładnikowe na ważnych kontach, korzystając z aplikacji takiej jak Aegis (getaegis.app) lub Jednostka autoryzacji (ente.com), a nigdy za pomocą SMS-ów (SMS jest podatny na włamanie do karty SIM).
Aby dowiedzieć się więcej, zapoznaj się z pełnym przewodnikiem dostępny tutaj.

Krok 6: Odzyskaj kontrolę nad swoimi urządzeniami

O tym właśnie zapomina wielu: szyfrujemy nasze wiadomości, ale mamy system, który nas szpieguje.
Na swoim komputerze przełącz się na **Linuksa** . Jest darmowy, nie szpieguje Cię i jest o wiele prostszy, niż myślisz. Najnowsze dystrybucje, zwłaszcza te z GNOME i KDE, są bardzo intuicyjne. Oprogramowanie jest łatwo dostępne, a nawet w przypadku gier wideo istnieją dystrybucje ze wszystkim, czego potrzebujesz, preinstalowane, na przykład CachyOS (cacheos.org) lub system operacyjny Steam (sklep.steampowered.com/steamos).
Na moim komputerze do gier Linux stał się moim domyślnym wyborem. Na początek Linux Mint (linuxmint.com) jest najprostszą dystrybucją i najbardziej zbliżoną do systemu Windows.

W przypadku telefonu najbardziej niezawodnym rozwiązaniem jest GrapheneOS (grapheneos.org). Jest to odtworzona i wzmocniona wersja Androida, którą można zainstalować na urządzeniu Google Pixel kilkoma kliknięciami z poziomu komputera.

To jest prawdziwe rozwiązanie, jeśli Twój telefon kiedykolwiek spróbuje Cię zeskanować lub podsłuchać Twoje rozmowy. Ponieważ jedynym sposobem na obejście tego typu inwigilacji jest zainstalowanie wersji Androida, która nie jest kontrolowana przez Google.
Aby dowiedzieć się więcej, zapoznaj się z pełnym przewodnikiem dostępny tutaj.

Krok 7: Aby pójść dalej

Jeśli chcesz osiągnąć maksymalną suwerenność: użyj **Tora**, aby oddzielić swoją aktywność od adresu IP, hostuj własne usługi na **YunoHost** lub **Umbrel** , uruchamiaj **lokalnie sztuczną inteligencję** zamiast wysyłać myśli do ChatGPT, a dla osób najbardziej narażonych na ryzyko zapoznaj się z zasadami anonimowości. Wszystko jest szczegółowo opisane krok po kroku w kompletnym przewodniku dostępnym tutaj: exitchatcontrol.org

Wniosek

Zmiana narzędzi jest aktem indywidualnej odpowiedzialności, unikalnym dla każdej osoby, co pozwala na sprzeciwienie się bezprawnej masowej inwigilacji.
Szyfrowanie danych chroni Twoją prywatność. Samodzielny hosting uwalnia Cię od inwigilacji ze strony firm technologicznych. Odzyskanie kontroli nad narzędziami czyni Cię niepodlegającym kontroli i suwerennym.
Walka ma charakter polityczny. Wesprzyj organizacje, które się jej sprzeciwiają, takie jak inicjatywa fightchatcontrol.eu
I napisz do swoich wybranych urzędników. To prawie doprowadziło do upadku Chat Control.
Ale ponieważ rozwiązania prawdopodobnie nie znajdziemy w głosowaniu ani w Parlamencie Europejskim, obowiązkiem każdego z nas jest wywalczenie wolności i ochrona prywatności przy użyciu wszystkich narzędzi udostępnionych w Internecie. *Pełny przewodnik, w którym wyjaśniono i zainstalowano krok po kroku każde narzędzie, od obywatela do sygnalisty, znajduje się tutaj* exitchatcontrol.org
Zapisz je, udostępnij i poproś bliskich o ich przeniesienie.
Niniejszy artykuł będzie aktualizowany w miarę rozwoju sytuacji.