Czas żeby się przygotować jest teraz!

Kiedy następuje eskalacja to nie ma już czasu ani przestrzeni emocjonalnej żeby się przygotować, dlatego zacznij już dziś! Polska sukcesywnie spada w rankingach wolności i demokracji[1], a także niezależności mediów[2], pytanie nie jest „czy" ale „kiedy" zacznie się blokowanie internetu[3] i rekwirowanie sprzętu. Dlatego właśnie potrzeba nam bezpiecznych kanałów komunikacji, maskowania ruchu w sieci czy budowania społeczności wokół wolnościowych serwisów.

nie ma czegoś takiego jak całkowite bezpieczeństwo

Bezpieczeństwo nie jest gotowym rozwiązaniem, a procesem opartym na minimalizowaniu ryzyka w oparciu o uważność i wyrabianie nawyków.

podstawy Kultury Bezpieczeństwa

Nawet, jeżeli wydaje ci się, że nie masz nic do ukrycia, pamiętaj, że materiały pozyskane przez służby specjalne i policję mogą zostać w taki sposób spreparowane, zmanipulowane i przedstawione, że nawet zupełnie niegroźne rzeczy odwrócą sens historii, która się faktycznie wydarzyła.[4]

- zakładaj, że wszystko, co trafia do sieci (również komórkowej) może stać się publiczne
- nie musisz wiedzieć wszystkiego, nie pytaj – bezpieczniej i dla Ciebie i dla innych
- jeśli wiesz, nie rozpowiadaj. Ty nie musisz być celem, możesz nieświadomie informować o innych
- anonimizuj wypowiedzi, nie rzucaj ksywami / imionami / nazwiskami
- usuwaj / niszcz wrażliwe informacje, gdy tylko przestają być Ci potrzebne

Szerzej temat podejmuje Anarchistyczny Czarny Krzyż w zinie *„O co chodzi w Kulturze Bezpieczeństwa?"*.[5]

skąd służby pozyskują dane

W Polsce jest 9 instytucji uprawnionych do prowadzenia tzw. czynności operacyjno-rozpoznawczych, są to m. in. Agencja Bezpieczeństwa Wewnętrznego i Policja. Wiemy, że operatorzy telekomunikacyjni przechowują (wyłącznie na potrzeby służb) informacje o tym, gdzie byliśmy w ciągu ostatnich 12 miesięcy i do kogo w tym czasie dzwoniliśmy, co przeglądaliśmy. Służby sięgają po te dane ponad milion razy w ciągu roku, bo są one dostępne od ręki, bez zezwoleń. Tak jak śledzenie.

Jednak poza tymi dwiema kategoriami większość działań służb jest tajemnicą: sprawdzają nas w rządowych rejestrach, mają zdalny podgląd do systemów monitoringu wizyjnego(w tym kamer rejestrujących tablice rejestracyjne na autostradach czy zapisujących adresy w sortowniach poczty), mogą „przyczepić komuś ogon". Mogą zbierać informacje o tysiącach z nas, np. poprzez sprawdzenie tożsamości właścicieli wszystkich telefonów, które były

[1] https://freedomhouse.org/report/freedom-world
[2] https://www.press.pl/tresc/65629,polska-coraz-nizej-w-rankingu-wolnosci-mediow
[3] https://rys.io/wypierdalac/netoobrona.md
[4] https://podsluchjaksiepatrzy.org/#inwigilacja
[5] https://pl.anarchistlibraries.net/library/crimethinc-o-co-chodzi-z-kultura-bezpieczenstwa

na proteście lub szczegółowo inwigilować wybrane osoby np. instalując na ich telefonach oprogramowanie szpiegowskie Pegasus (co jest dość drogim rozwiązaniem). A szef ABW może założyć podsłuch bez konieczności uzyskania zgody sądu, jeśli podejrzewa kogoś o terroryzm.

Jeśli policja chce założyć ci podsłuch, musi prosić o zgodę sąd, jednak to tylko formalność - 99% wniosków jest rozpatrywanych pozytywnie. Rocznie polska policja zakłada 8–10 tysięcy podsłuchów, co daje 25 dziennie. Pozostałe służby w samym 2019 r. podsłuchiwały 1267 osób. Zgoda na podsłuch to jedyna sytuacja, w której policjant musi prosić o pozwolenie.[6]

Polskie służby pytają też o dane Facebooka, w 2019 r. zrobiły to 10 tys. razy, to 100% więcej niż rok wcześniej, w około połowie przypadków je dostają.[7] Facebook ma też własne algorytmy do wykrywania niepożądanych zachowań i może na tej podstawie zgłaszać się do policji (wykrywanie handlu narkotykami w usa).

kluczowa rola osobowych źródeł informacji

Niemożliwe? A jednak! Nadal łatwiej jest służbom zdobywać informacje od ludzi niż łamać zabezpieczenia sprzętu. 76,21% badanych policjantów najczęściej korzysta z pomocy osób informujących[8] (czyli tzw. kretów / wtyk / konfidentów / informatorów). Historycznie są znane przypadki sterowania ruchami społecznymi przez agentów. Ponadto służby mogą czerpać informacje z przesłuchań i czynności (cały ten czas po zatrzymaniu) wykorzystując przy tym rozbudowane metody manipulacji.[9]

jak daleko służby mogą się posunąć?

[TW: przemoc]

Niejaki Mark Stone, od wielu lat zaangażowany w radykalne skrzydło ruchu, organizator demonstracji, okupacji i pikiet (m.in. przeciwko szczytowi grupy G8 w Szkocji), okazał się policyjną wtyką. Wzbudził podejrzenia, gdy znajoma działaczka w trakcie wspólnych wakacji zobaczyła jego paszport, w którym widniało nazwisko Kennedy zamiast Stone. Mark Kennedy prowadził podwójne życie. Wchodził w romantyczne relacje z działaczkami. (…) Kolejne śledztwa ujawniły serię wątpliwych etycznie działań brytyjskich służb. Szpiegów było więcej. Za wiedzą przełożonych, w czasie pracy, wykorzystywali seksualnie niczego nieświadome aktywistki. Byli ojcami ich dzieci. Zdarzało się, że kończąc „misję" znikali z ich życia.

Fakt, że policyjni szpiedzy faktycznie współorganizowali, prowokowali część niezgodnych z prawem działań ruchu ekologicznego, doprowadził do wycofania zarzutów wobec osób zaangażowanych w nieudaną akcję zablokowania elektrowni węglowej Ratcliffe-on-Soar w Nottinghamshire. [10]

Stone/Kennedy był też w polsce w ramach infotouru G8 w Rostoku, razem z drugą policjantką i nieświadomym aktywistą, był odpowiedzialny za logistykę aktywistów na G8 w Szkocji i infiltrował wiele różnych grup. Służby nie ograniczą się tylko do tych grup, które sprawiają wrażenie groźnych, inna funkcjonariuszka infiltrowała np. CIRA (grupę klaunów).

[6] https://podsluchjaksiepatrzy.org/#inwigilacja
[7] https://panoptykon.org/jak-bezpiecznie-protestowac
[8] K. Horosiewicz, Współpraca policjantów z osobowymi źródłami informacji, Warszawa 2015
[9] http://szkolenia.policja.waw.pl/wdz/informacje/psychologia/27370,Zasady-przesluchania-metoda-FBI.html
[10] https://krytykapolityczna.pl/kraj/pegasus-inwigilacja-ruchow-ekologicznych/

Opór - od czego zacząć?

Ten poradnik nie powstał z intencją wzbudzenia w Tobie paraliżującego strachu a raczej motywującego do działania niepokoju. Czytając poniższy tekst poznasz konkretne narzędzia, które pomogą Ci zadbać o prywatność i podnieść poziom bezpieczeństwa, zarówno Twój jak i grup, w których działasz.

zahasłuj telefon

Po pierwsze wyłącz odblokowanie odciskiem palca czy skanem twarzy, które w przypadku konfiskaty sprzętu dość łatwo zdobyć przy użyciu siły. Najlepsza jest blokada przy pomocy rysowanego kodu (łączenia kropek), bo ma wiele kombinacji. Pin też jest dobrym pomysłem, jednak bardziej uciążliwym, żeby był bezpieczny powinien się składać z minimum 10, a rekomendowane jest 13 cyfr. 4 cyfrowy kod można bezproblemowo złamać testując po kolei konfiguracje – przy pomocy komputera.[11]

szyfruj wiadomości i połączenia

Signal[12] i Element (dawniej Riot)[13] to sprawdzone, proste i względnie bezpieczne komunikatory, które polecamy. Są dwie zasadnicze różnice - Signal wymaga podania i udostępniania osobom, z którymi rozmawiasz, numeru telefonu, podczas gdy Elementowi wystarczy mail. Za to Signal w odróżnieniu od Elementu, domyślnie szyfruje również konferencje grupowe. Pamiętaj, że nawet szyfrowany komunikator nie uchroni Cię, jeśli np. jest sczytywany ruch z Twojej klawiatury – przed zaszyfrowaniem treści (a jest dopóki nie wymienisz jej na opensourceową i bezpieczną) lub masz zhakowany telefon (pegasus).

Mniej atrakcyjny wizualnie, ale przydatny na demonstracjach (jeśli zabierasz na nie telefon;) jest Briar, który pozawala komunikować się przy pomocy bluetootha – czyli nawet, gdy występują problemy z siecią komórkową, jego wadą jest brak aplikacji na iphony. Większość pozostałych służy głównie do zbierania danych na nasz temat, sprzedawanych komukolwiek, kto zapłaci. Mowa tu zwłaszcza o Messengerze, Telegramie, Viberze, Discordzie, czy Skypie. Tych rozwiązań należy unikać, zwłaszcza gdy rozmawiamy na tematy wrażliwe, chociaż wtedy najlepiej w ogóle nie mieć przy sobie elektroniki.

Signal to komunikator, który może zastąpić domyślną aplikację do wiadomości (smsów) na smartphonie, ma również wersję na komputer. Do normalnych kontaktów wysyła SMSy, do osób, które też mają Signala wysyła silnie szyfrowane wiadomości w sposób, który podnosi anonimowość komunikacji. Umożliwia przesyłanie grafik, plików i wiadomości głosowych, czy lokalizacji, oraz tworzenie grup. Do ciekawych funkcji należą też znikające wiadomości, oraz maskowanie twarzy na zdjęciach, jeśli tylko tego chcemy. Z powodzeniem wykorzystywany jest przez niektóre grupy, jako platforma do natychmiastowej komunikacji, chociaż przy masowych demonstracjach warto pamiętać, że sieć GSM może być po prostu przeładowana i nie zawsze można na niej polegać. Jest to też open, source, więc wszyscy mają możliwość dokładnej analizy zabezpieczeń i aktywnego uczestnictwa w poprawianiu programu.

[11] https://panoptykon.org/jak-bezpiecznie-protestowac
[12] https://signal.org/pl/download/
[13] https://element.io/

Sam w sobie, nie jest jednak gwarantem bezpieczeństwa, czy anonimowości. Niemniej, to prosty pierwszy krok w dobrym kierunku. Znajomo wyglądający interfejs i prostota użycia sprawiają, że może go używać każda osoba. Im będzie ich więcej, tym mniej informacji na nasz temat może być w stanie gromadzić operator sieci i inne mroczne siły. Według prawa operatorzy mają obowiązek trzymać każdą przesłaną wiadomość przez rok.[14]

nie trzymaj na telefonie nadmiaru danych

Zazwyczaj telefon jest kopalnią wiedzy o osobie, która go używa. Dzieje się tak, bo wielu osobom sprzęt ten towarzyszy nieustannie, z czym wiążą się kolejne zagrożenia np. utraty, wtedy lepiej żeby na urządzeniu było jak najmniej danych. Żeby zminimalizować ryzyko przejęcia wrażliwych informacji przez niepożądane osoby:

- często zgrywaj zawartość telefonu
- włącz *znikające wiadomości* (funkcja Signala) - wiadomość przestaje być dostępna po określonym czasie
- pamiętaj, że domyślnie zewnętrzne karty pamięci **nie** są szyfrowane!
- sprawdź, jakie informacje zbierają o Tobie poszczególne aplikacje, może czas zmienić ich uprawnienia lub poszukać alternatyw?

[14] https://szmer.info/post/3437

regularnie aktualizuj system i aplikacje

Zapewnisz sobie tym samym naprawianie luk w zabezpieczeniach i szyfrowanie zawartości telefonu (na IOS na Androidzie od 5 jest to domyślne i automatyczne, we wcześniejszych wersjach Androida szyfrowanie trzeba włączyć ręcznie w ustawieniach).

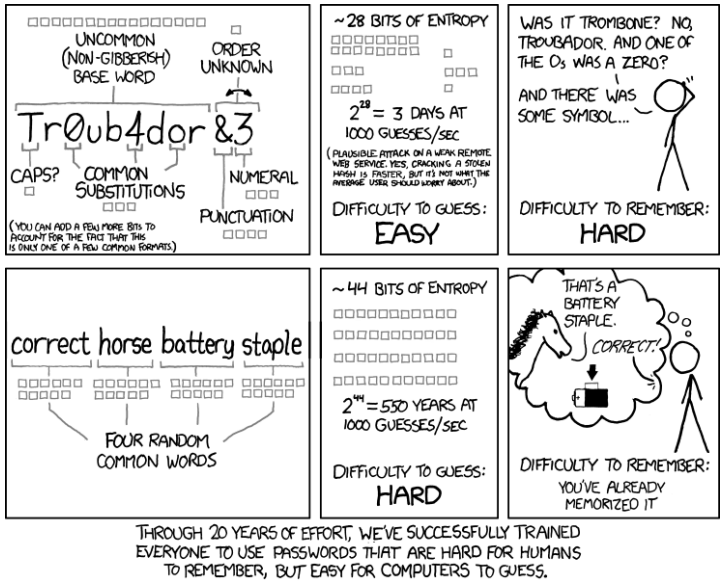
Aktualizowanie systemu komputera również zapewnia naprawianie luk w zabezpieczeniach (czyli też antywirusach i firewallach, które obecnie są wbudowane w systemy operacyjne).

hasła

Jeśli dojdzie do wycieku danych, z jakiejś strony, na której założyłeś konto 5 lat temu i użyłeś go tylko wtedy, ale użył*ś tam hasła takiego jak do maila, to ktoś może przejąć kontrolę nad praktycznie wszystkimi Twoimi kontami korzystając z opcji „zapomniał*m hasła”. Dlatego nie powtarzaj tych samych haseł w różnych miejscach. Stosowanie kombinacji tego samego hasła nie jest rozwiązaniem, poznając jedną z modyfikacji łatwo jest odgadnąć kolejne.

Jak tego uniknąć?

Ułóż 4 zdania zawierające wielkie litery i interpunkcję, każde składające się z 4-5 słów. Nic więcej nie musisz zapamiętywać! A tym bardziej skomplikowanych ciągów znaków, a Twój poziom ochrony jest wyższy.



- Zdanie pierwsze będzie Twoim hasłem systemowym (do zalogowania się do komputera).
- Zdanie drugie będzie hasłem do odszyfrowania dysku (o tym później).
- Zdanie trzecie będzie hasłem do maila.
- A zdanie czwarte do menadżera haseł, o czym poniżej.

Menadżer haseł to program / aplikacja, która tworzy szyfrowaną bazę danych z informacjami, o tym gdzie masz ustawione, jakie hasło. Za pomocą menadżera możesz generować skomplikowane hasła, składające się ze wszystkich dostępnych alfabetów, znaków specjalnych i cyfr – praktycznie niemożliwe do złamania.

Polecanym przez nas jest **KeePassXC**, m. in. dlatego, że:

- dostępna jest wtyczka do Mozilli i Chromium automatycznie zaciągająca z niego hasła
- działa offline
- działa na Windowsie, Linuksie i Macu
- ma wersję na Androida oraz iOS
- oferuje mocne algorytmy szyfrowania
- otwartoźródłowy (unikniemy podejrzeń o ingerencje służb w kod)
- darmowy[15]

Pamiętaj: nie zapisuj haseł w przeglądarce!

korzystaj dwuskładnikowego uwierzytelniania

W serwisach, które oferują tę opcję korzystaj z możliwości dwuskładnikowego uwierzytelniania, to dodatkowy poziom bezpieczeństwa dla kont internetowych, oprócz loginów i haseł. Aby mieć generator kodów w jednym miejscu skorzystaj z FreeOTP. To darmowa, open-sourceowa apka na telefon, służąca do generowania jednorazowych, wygasających po chwili kodów do dwuetapowego uwierzytelniania kont internetowych. Kody mogą być dodane albo skanując kod QR lub manualnie. Wygenerowane kody są unikalne i ważne jedynie przez chwilę, więc bardzo trudno jest zhakować. Są one wygenerowane nawet, jeśli telefon jest w trybie samolotowym.

[15] https://niebezpiecznik.pl/post/keepass-jak-zaczac-swoja-przygode-z-managerem-hasel/

nie klikaj w nieznane linki

Łatwiej zdobyć dostęp do Twojego sprzętu socjotechniką niż łamiąc zabezpieczenia. W związku z tym możesz dostawać na pozór niewzbudzające podejrzeń wiadomości (maile / smsy), zdarzały się nawet telefony – element zaskoczenia i trochę manipulacji potrafi skłonić człowieka do podania hasła. Częściej jednak ma to bardziej przyziemny wymiar i przez własne roztargnienie czy nieuwagę osoby klikają w niebezpieczny link, może skutkować utratą kontroli nad sprzętem i danymi.

szyfruj dysk komputera

Zaszyfrowanie dysku to rozwiązanie, które chroni zawarte na dysku informacje. Szyfrowanie to nic innego jak zmiana zawartości dysku w niezrozumiały kod, który można rozszyfrować tylko podając hasło. Oznacza, to że bez podania hasła jego zawartość jest bezużyteczna.

Chociaż szyfrowanie dysku może zależeć od systemu operacyjnego to uniwersalnym rozwiązaniem jest VeraCrypt (dla IOS i Windowsa rekomendowanym). Linux zazwyczaj ma wbudowane szyfrowanie dysku, które jest opensourcowe jak sam system. iOS ma opcję FileVault, która szyfruje dysk, ale automatycznie synchronizuje hasło do odszyfrowywania z hasłem systemowym. Windows udostępnia opcję szyfrowania dysku tylko we wersjach profesjonalnych, dopiero po zalogowaniu do konta Microsoft, dodatkowo Twój klucz do odszyfrowania jest trzymany na serwerach Microsoftu (co podważa jakiekolwiek bezpieczeństwo).

stwórz bezpieczną kopię

Zaszyfrowane pliki trzymaj na dysku zewnętrznym lub w bezpiecznej chmurze. Pamiętaj żeby często aktualizować zwartość kopii zapasowej, w razie utraty sprzętu stracisz tylko niewielka część danych.

sytuacje awaryjne

W przypadku chęci szybkiego zabezpieczenia sprzętu (np. w przypadku wizyty służb) masz dwa wyjścia:

- wyłączyć komputer przyciskiem zasilania - zabezpieczy go to przed dostępem osób trzecich, ale jednocześnie może go zniszczyć
- zablokować ekran skrótem klawiszowym – łatwiejszy do odblokowania ale bez ryzyka uszkodzenia sprzętu, jeśli zamierzasz korzystać z tej opcji zapisz sobie kombinację klawiszy w widocznym, z perspektywy osoby siedzącej przy komputerze, miejscu.
  - ✓ dla Windowsa: Windows + L
  - ✓ dla Maca: Option + Shift + Command + Q
  - ✓ Linux: CTRL + ALT + L lub Windows + L

W stresie nawet standardowe czynności wydają się skomplikowane.

używaj open sourcowych alternatyw

open source — oprogramowanie z dostępnym dla każdego kodem źródłowym, dzięki czemu mogą być on zmieniany, udoskonalany i rozpowszechniany, co pociąga za sobą szybki rozwój programów.

Dlaczego uważamy, że kod źródłowy programów / narzędzi musi być otwarty? Bo tylko wtedy jest możliwy do zweryfikowania, pozwala to ekspertom i ekspertkom przeprowadzić testy i zweryfikować czy program jest tym, za co się podaje.

Dobrze to zagadnienie obrazuje przykład ANoM – telefonu, który był sprzedawany, jako bezpieczny, oparty na modyfikacji Androida z wbudowaną aplikacją do szyfrowania komunikacji, brzmi super? Jak się okazało urządzenia te nie stały na Androidzie tylko własnym systemie, zostały wprowadzone na rynek przez FBI a dalej rozdystrybuowane przez jednego ze skazanych, który „rekomendował" je w zamian za obniżenie wymiaru kary. Nie zweryfikowano kodu systemu ani aplikacji, tym sposobem światek przestępczy komunikował się na kanałach, które przygotowały dla niego amerykańskie służby.[16]

Open sourcowe programy i apki:

Linux[17] jest rodziną systemów operacyjnych, prawdopodobnie najbardziej przystępną wersją dla osoby użytkującej będzie ubuntu, do której instalacji jest dostępny obszerny poradnik w języku polskim[18]. Bardziej skupione na bezpieczeństwie są Tails i CubesOS, raczej dla osób bardziej zaawansowanych technicznie.

Mozilla Firefox to przystępna i działająca na każdym systemie (również urządzeniach mobilnych) przeglądarka. Ma wiele rozszerzeń, które pomogą Ci zadbać o komfort przeglądania internetu i podniosą bezpieczeństwo. Jakie wtyczki warto dodać?

- uBlock Origin[19] - blokuje reklamy (również dźwiękowe), ma dużo dodatkowych filtrów do polskiego internetu[20]
- https everywhere[21] - dba żeby Twoje połączenie ze stroną było szyfrowane
- Privacy Badger[22] - blokuje elementy śledzące Twoją aktywność w internecie
- KeePassXC Browser[23] – automatycznie zaciąga hasła z menadżera, gdy mamy otwartą bazę haseł

Programy biurowe, takie jak Miscrosotf Office możesz zastąpić Libre[24] lub Calligrą[25], która oferuje nawet więcej możliwości niż wspomniany korpo pakiet.

Jeśli potrzebujesz klienta do odbierania poczty możesz skorzystać z ThunderBirda[26].

Aplikacje do wideokonferencji takie jak zoom czy skype, można zastąpić jitsi[27] (dostępne w przeglądarce, bez rejestracji, ma też aplikację na iOS i Androida) lub Signal (dostępny również na komputer).

[16] https://szmer.info/post/5767, http://blogotech.eu/index.php/11728-anom-spreparowany-telefon-dla-przestepcow
[17] https://www.linux.org/pages/download/
[18] http://ubuntu.pl/dokumenty/Przewodnik_Ubuntu_14.04_LTS_Trusty_Tahr.pdf
[19] https://addons.mozilla.org/pl/firefox/addon/ublock-origin/
[20] https://majkiit.github.io/polish-ads-filter/
[21] https://www.eff.org/https-everywhere
[22] https://www.eff.org/pages/privacy-badger
[23] https://addons.mozilla.org/pl/firefox/addon/keepassxc-browser/
[24] https://www.libreoffice.org/download/download/
[25] https://calligra.org/download/
[26] https://www.thunderbird.net/pl/
[27] https://meet.jit.si/

F-droid to alternatywa sklepu play, tylko że są w nim same z otwarto-źródłowe apki, udostępnione za darmo.

oprogramowanie / programy

korpo	open source
windows, macOS	linux (np. ubuntu)
chrome, chromium, safari	mozilla firefox, librewolf, falkon
office	libre, calligra
outlook	thunderbird
zoom, skype	jitsi, signal

serwisy

korpo	open source
gmail, hotmail, wp poczta, onet poczta, interia, o2	disroot, protonmail,
facebook	friendica, pleroma
facebookowe event	radar squat net, mobilizon
instagram	pixelfed
twitter	mastodon
youtube	peertube
reddit, wykop	szmer, lemmy
google	searX, qwant
google maps	open street maps
google driver / google suit	nextcloud, riseup, disroot

Część serwisów[28] wymienionych w tabelce stanowi Fediwersum (*fediverse* — federated universe — *sfederowane uniwersum*) - sieć niezależnie funkcjonujących sieci społecznościowych, wzajemnie się ze sobą komunikujących.[29] Widzisz w nich to co wrzucają konta, które obserwujesz, a nie to co wybiorą Ci szpiegujące algorytmy nastawione na zysk.
Platformy do organizacji, udostępniania i organizowania się:

- disroot.org – mail, chat, chmura, forum, pady, arkusze kalkulacyjne itp.
- riseup.net – mail, forum, grupy robocze, listy zadań itp.

Na disroocie nie potrzebujesz zaproszenia, żeby założyć maila (w odróżnieniu od riseup.net).

Więcej otwarto źródłowych programów i apek znajdziesz tu:

- https://switching.software/
- https://alternativeto.net/
- https://osalt.com/

przeglądarka TOR (The Onion Routing)

Tor Browser zapewnia anonimowość w sieci poprzez ukrywanie adresu IP użytkownika, omija cenzurę internetu umożliwiając użytkownikom dostęp do zablokowanych stron i/lub witryn internetowych, nie zawiera domyślnych funkcji śledzenia online, nie zarabia na wykorzystywaniu danych użytkowników. Uniemożliwia zdobycie informacji o stronach internetowych, które odwiedzasz, przez kogoś monitorującego twoje połączenie internetowe, a także uniemożliwia odwiedzanym stronom poznanie Twojej fizycznej lokalizacji. Tor to sieć rozproszona, dlatego jest bardzo trudna do zablokowania.

[28] https://fediverse.pl/poznaj-alternatywy/

[29] https://fediverse.pl/jak-dziala-fediwersum/

Przesyłane informacje mogą być jawne, w przeciwieństwie do ich źródła, dlatego tak ważne jest, aby korzystając z TORa nie wysłać danych na swój temat, szczególnie danych osobowych, takich jak nazwisko, adres, urodziny, numer karty kredytowej. Aby pozostać całkowicie anonimową, nie należy logować się na żadne strony, które tego wymagają.

TOR zapewnia:

- blokowanie trackerów — przeglądarka separuje każdą odwiedzaną stronę internetową, aby trackery i reklamy osób trzecich nie mogły Cię śledzić. Wszelkie pliki cookie są automatycznie usuwane po zakończeniu przeglądania. Tak samo jak historia przeglądania. Trackery zbierają informacje o stronach internetowych, które odwiedzasz, a także informacje o Twoich urządzeniach.
- obrona przed nadzorem - Tor Browser zapobiega sytuacji, w której ktoś obserwujący Twoje połączenie wie, jakie strony odwiedzasz. Ktoś monitorujący twoje nawyki przeglądania może zobaczyć, to że używasz Tor.
- odporność na zjawisko fingerprintingu — Tor dąży do tego, aby wszyscy użytkownicy wyglądali tak samo, co utrudnia ich rozpoznanie. „Odcisk palca" to informacje o Twojej przeglądarce i sprzęcie, na podstawie, których można (lub nie) Cię zidentyfikować – mogą być unikatowe, ale lepiej żeby nie były. Możesz to sprawdzić tutaj: https://coveryourtracks.eff.org/
- wielowarstwowe szyfrowanie — Twój ruch jest przekazywany i szyfrowany trzykrotnie podczas przechodzenia przez sieć Tor.

Korzystanie z TOR-a może być widoczne dla operatora Twojej sieci, jeśli takiej informacji poszuka, domyślnie się nie wyróżnia spośród innych szyfrowanych połączeń.

Nie używaj wtyczek ani dodatków — paczka Tora z przeglądarką zawiera kilka dodatków, takich jak HTTPS Everywhere i NoScript, z których wszystkie są bezpieczne w użyciu i zwiększają twoją anonimowość. Aby zachować bezpieczeństwo, nie należy dodawać kolejnych.

VPN (Virtual Private Network)

Gdy łączysz się z siecią VPN, wszystkie dane, które wysyłasz (takie jak żądania do serwerów podczas przeglądania stron internetowych), z perspektywy strony czy usługi mają źródło z serwera VPN, a nie twojego dostawcy usług internetowych. Maskuje to twój adres IP, który wraz z informacją o Twoim dostawcy internetu, wskazuje na dokładną lokalizację.

VPN chroni Twój ruch internetowy przed inwigilacją w sieci publicznej, ale nie chroni Twoich danych z sieci prywatnej, z której korzystasz. Jeśli korzystasz z korporacyjnej sieci VPN, to ktokolwiek zarządza siecią korporacyjną, będzie widział Twój ruch. Jeśli korzystasz z komercyjnej sieci VPN, ten, kto zarządza usługą, będzie mógł zobaczyć Twój ruch.

W wolnej cenie możesz korzystać z VPN Riseupa[30] ale w dobrym tonie jest nie wykorzystywanie go do oglądania śmiesznych kotów w internecie ;) W przeciwieństwie do większości dostawców VPN Riseup nie rejestruje Twojego adresu IP. Jest super łatwy w użyciu. Po prostu instalujesz go i uruchamiasz — bez konfiguracji, bez rejestracji konta.

Można też postawić sobie własny VPN używając względnie prostych rozwiązań takich jak yunoHost.

[30] https://riseup.net/pl/vpn

wsparcie

Z pewnością nie udało się tutaj wyczerpać tematu, poza tym technologie nieprzerwanie się rozwijają a edukacja jest procesem. Możesz dalej eksplorować powyższe zagadnienia np. na stronie Fundacji Panoptykon[31] czy w szmerowych społecznościach takich jak *cyberbezpieczeństwo*[32], *wolny internet*[33] czy *hakt*[34], znajdziesz tam też spis praktycznych porad technicznych[35]. Kwestie związane z uprawnieniami służb znajdziesz w dedykowanej społeczności[36]. Są też portale branżowe takie jak niebezpiecznik czy sekurak jednak dość nachalnie oferują swoje szkolenia.

Dla wielu jednak będzie to duża dawka wiedzy, która może powodować poczucie zagubienia. Jeśli masz jakieś wątpliwości, napotkasz problemy z instalacją lub jeszcze coś innego możesz skorzystać z kolektywnej wiedzy szmerowych nerdów i nerdek (bez których ten poradnik by nie powstał!) w społeczności *zapytaj Szmer*[37].

Dzięki za zainteresowanie i chęć budowania bardziej wolnościowego internetu!

[31] https://panoptykon.org/wiedza
[32] https://szmer.info/c/cyberbezpieczenstwo
[33] https://szmer.info/c/wolnyinternet
[34] https://szmer.info/c/hakt
[35] https://szmer.info/post/2890
[36] https://szmer.info/c/policja
[37] https://szmer.info/c/zapytajszmer

notatki