Poradnik unikania inwigilacji[1]

prof. dr hab. Dariusz Jemielniak[2]

Ustawa o inwigilacji obywateli (nowelizacja ustawy o policji) zwiększyła ogólne zainteresowanie społeczne tematyką zabezpieczeń urządzeń elektronicznych. Jednocześnie większość z nas nie ma głowy, doświadczenia i czasu, aby wczytywać się w detale techniczne i samodzielnie wybierać aplikacje, które pomogą nam w ochronie przed niepożądaną inwigilacją, kradzieżą danych, itp. Niniejszy krótki poradnik wskazuje na subiektywnie wybrane najlepsze aplikacje, których użycie znacznie utrudni inwigilację nietargetowaną (tj. np. masowy podsłuch rozmów i SMSów, bez koncentrowania się na konkretnej osobie). Starałem się wybrać aplikacje, które są stabilne, znane i użyteczne – a także nie proponować ich dużej liczby (przykładowo, rekomenduję Signal, a nie Telegram, czy Tox i nie wchodzę już w szczegóły, dlaczego Signal uważam za najsensowniejszy).

Proszę pamiętać, że zastosowanie poniższych rozwiązań pomaga jedynie technicznie, a nie społecznie – czyli nie zwalnia nas z konieczności stosowania dobrych praktyk (nieotwieranie niezapowiedzialnych załączników i podejrzanych linków, zwłaszcza od mniej znanych osób; nieinstalowanie zbędnych aplikacji od niezaufanych producentów; unikanie używania *pendrive* USB). Zarówno komputer, jak i telefon, powinny być wyposażone w aktualne oprogramowanie antywirusowe.

Trzeba też pamiętać, aby nie używać tych samych haseł do różnych serwisów, a także wybierać hasła, w których nie będzie fragmentów słów, a także będą kombinacje liter (dużych i małych), cyfr i znaków specjalnych. Dobrą mnemotechniką jest np. wybranie zwrotki z ulubionej piosenki i oparcie hasła na niej, np. „Świat nie wierzy łzom, w życiu tak już jest", możemy przerobić na łatwe do zapamiętania hasło „Snw1wztjJ!". Niezłym rozwiązaniem jest też korzystanie np. z menedżerów haseł, jak LastPass.com, czy 1Password na komputerze i telefonie (pełna wygoda na wszystkich urządzeniach niestety wymaga często prenumeraty, dlatego polecam alternatywnie całkowicie darmowy i open source Password Safe lub KeePass). W każdym serwisie, gdzie możliwa jest tzw. dwustopniowa autoryzacja (za pierwszym razem, jak się logujemy z nowego urządzenia, musimy to potwierdzić kodem), należy ją uruchomić - dzięki czemu sama utrata hasła jest mniej groźna. Instrukcje, jak to włączyć: Dropbox, Facebook, Google, Apple.

Koncentruję się na głównych zagrożeniach inwigilacji, ale nie na reklamach, czy trackingu przez korporacje – dlatego pomijam Adblocka, Adblock Plus, Privacy Badger, uMatrix, czy Ghostery, choć również zachęcam do ich przejrzenia.

Okazjonalnie proponuję alternatywy – jednakże osoba, która nie lubi wybierać, w ciemno może skorzystać z dowolnego rozwiązania w danej kategorii.

Jak zwrócił mi uwagę Tomasz Tarchała, w wielu korporacjach panuje obyczaj wymagania instalacji certyfikatu, aby móc korzystać z Wifi. Trzeba pamiętać, że naraża to nas na inwigilację także w połączeniach przez https - więc w skrócie, jeżeli musicie coś takiego instalować, do poufnych transferów wyłączajcie wifi (i korzystajcie z 3G/4G), a w ogóle to przede wszystkim zawsze używajcie VPN (o którym niżej) do poufnych danych lub gdy korzystacie z publicznie dostępnych wifi.

[2] profesor w NeRDS (New Research on Digital Societies) w Akademii Leona Koźmińskiego, fellow na Berkman Center for Internet and Society (Harvard), visiting scholar na MIT, członek Rady Powierniczej Fundacji Wikimedia, aktywista ruchu wolnej informacji.

Na komputerze

Przeglądarka Tor https://www.torproject.org/projects/torbrowser.html.en Program na Windows, Mac, Linux – jest wersja polskojęzyczna	Program na Windows, Mac, Linux – jest wersja polskojęzyczna Wykorzystanie tej darmowej przeglądarki uniemożliwia śledzenie witryn, jakie odwiedzamy przez pośrednika (czyli np. przez dostawcę internetu). Utrudnia też stronom ustalenie, gdzie jesteśmy. Warto pamiętać, że jeżeli surfujemy z przeglądarki, w której jesteśmy np. zalogowani na konto Google, informacje o naszych wyszukiwaniach będą rejestrowane przez tę firmę (dlatego jeżeli zależy nam na anonimowości wyszukiwań, powinniśmy używać np. DuckDuckGo). Warto też zdawać sobie sprawę, że ponieważ Tor kieruje nasz ruch przez różne kraje, np. dla Facebooka czy Google może to się wydać podejrzane i prewencyjnie zablokują konto - tym bardziej warto mieć logowanie dwuetapowe, o którym piszę wyżej. Facebook jednak wychodzi naprzeciw użytkownikom Tor, od niedawna także łączy się z Orbotem na urządzeniach z Androidem (o aplikacji Orbot niżej, w części dla telefonów).
Https Everywhere https://www.eff.org/Https-Everywhere Wtyczka do Chrome, Firefox, Opera	Wtyczka do standardowych przeglądarek, wymuszająca połączenie szyfrowane (w skrócie, chodzi o to, że wiele serwerów umożliwia je, ale nie domyślnie, wtyczka ta ułatwia nam życie).
VPN Serwisy zabezpieczające połączenie	Usługa zabezpieczające połączenie. Użycie VPN powoduje, że dostawca usługi i wszelcy pośrednicy nie wiedzą, jaki rodzaj danych jest przesyłany – czy to film, czy dokument tekstowy, czy coś innego (o treści nie wspominając). Usługi VPN są, w przeciwieństwie do Tor, płatne – warto jednakże rozważyć instalację na stałe serwisu VPN, zwłaszcza, jeżeli bardzo istotny jest dla nas komfort wysokiej szybkości połączenia. Każdy musi wybrać taką, jaka mu pasuje (także cenowo, dobra cena to ok. 2-5$ miesięcznie, ale i pod względem wielu różnych czynników - tutaj zestawienie ponad stu VPN, tu z kolei najlepsze VPN wg PCMag na 2016), trzeba jednak pamiętać, że niektóre serwisy VPN (np. popularny „Hide My Ass") przetrzymują logi i udostępniają dane agendom rządowym. Sam używam CactusVPN (z uwagi na kombinację ceny, łatwości instalacji, a także dostępności na telefon komórkowy bez dodatkowych opłat), polecane są też choćby VyprVPN, czy .
Opcjonalnie: **CryptoCat** https://crypto.cat/ Wtyczka do Chrome, Safari, Firefox, Opera, aplikacja iOS	Wtyczka, która umożliwia przesyłanie plików w sposób bezpieczny, w przyszłości także w integracji z chatem Facebooka.
Bitlocker Funkcja Windows **FileVault** Funkcja MacOSX	W zależności od wersji systemu operacyjnego Windows, czasami możemy darmo skorzystać z funkcji szyfrowania dysku BitLocker (Windows 10, 8.1 Pro/Enterprise i in.) – jeżeli mamy tę funkcję, trzeba ją włączyć! (Panel sterowania -> System i zabezpieczenia -> Szyfrowanie dysków), choć pomoże to bardziej przeciw kradzieży danych, niż inwigilacji (służby poradzą sobie). Użytkownicy Mac powinni włączyć funkcję FileVault. Lepszą alternatywą jest darmowy i open source program VeraCrypt (Windows, MacOSX, Linux). Jest on zdecydowanie nieoceniony także wtedy, gdy używa się kilku różnych systemów i chce np. szyfrować dysk zewnętrzny. Znam ekspertów od zabezpieczeń, którzy chwalą sobie także płatny Symantec Drive Encryption. Do wygodnego szyfrowania pojedynczych plików można użyć darmowego AxCrypt. Uwaga na temat telefonów - o ile użytkownicy iPhone mają domyślnie włączone szyfrowanie danych, o tyle na Androidzie robią tak tylko niektóre telefony (np. Nexus 6 i późniejsze), dlatego trzeba sprawdzić,

	czy opcja ta jest włączona w ustawieniach zabezpieczeń telefonu.
Opcjonalnie: **SpiderOak** https://spideroak.com Aplikacja na WIndows, Linux, MacOSX, Anroid, iOS	Wielu z nas używa dysków w chmurze (Dropbox, Google Drive, OneDrive). To wygodne, choćby do backupów, ale niestety mało chroni dane. Lepszym rozwiązaniem jest SpiderOak, który służy jako bezpieczny dysk chmurowy, ale jest, niestety od zeszłego roku płatny (60 dni darmowego testowania 2GB). Uwaga: proszę nie nabierać się na polecaną przez spidersweb.pl chmurę Mega (50 GB darmo) - sam jej twórca przyznaje, że dane nie są tam bezpieczne.
Opcjonalnie: **Viivo** https://viivo.com/ Aplikacja na WIndows, MacOSX, Anroid, iOS	Osoby, które chcą korzystać z dysków chmurowych, ale nie chcą ich zmieniać (choćby dlatego, że mają je darmo), powinny zainstalować program do szyfrowania plików w chmurze. Polecam Viivo lub Boxcryptor (ten ostatni – płatny powyżej dwóch urządzeń).

Na telefonie

Signal https://whispersystems.org/ Aplikacja na Androida i iOS	Aplikacja zastępująca domyślny program do SMSów, umożliwiająca także bezpośrednie rozmowy telefoniczne. Wszystko jest szyfrowane po stronie klienta: inaczej mówiąc, w przeciwieństwie do zwykłego telefonu, nie da się łatwo podsłuchać rozmowy ani treści SMSów, o ile obie strony mają zainstalowany Signal. Signal jest bardzo łatwy w użyciu, ma przejrzysty interfejs, kod open-source poddawany audytom i polecany przez ekspertów - jego jedyną wadą jest posiadanie centralnego serwera, dlatego warto go używać w połączeniu z Orbot lub VPN. Wersja beta jest też dostępna na komputery stacjonarne. *Uwaga dla bardziej wtajemniczonych:* programów tego typu jest stosunkowo sporo. Signal ma jedne z najlepszych rozwiązań kryptograficznych na świecie i bardzo wysoką wygodę użycia, nadaje się nawet dla początkujących użytkowników, a także załatwia na raz kwestię SMSów i połączeń, dlatego zdecydowanie polecam właśnie ten standard, a nie któryś z licznych innych, jak Tox, Telegram, czy Lumicall i SMSSecure. Mocno zaawansowanym użytkownikom o bardzo wysokich potrzebach zabezpieczeń ewentualnie polecam Vuvuzelę (ale oni nie potrzebują tego poradnika). Oczywiście uparci mogą wybierać inny standard i przekonywać wszystkich znajomych do niego, w końcu wartość danego programu rośnie wraz z liczbą używających go osób. Zdecydowanie nie warto natomiast podążać za poradami, wygłaszanymi nawet przez całkiem poważne serwisy, jak spidersweb.pl, aby polegać w tej kwestii na WhatsApp. WhatsApp nie gwarantuje nam takiego samego poziomu bezpieczeństwa, jak Signal - zachęcam do lektury zestawienia Electronic Frontiers Foundation.
Orbot https://play.google.com/store/apps/details?id=org.torproject.android Aplikacja na Androida	Program umożliwiający tunelowanie ruchu dla wybranych aplikacji przez sieć Tor. W najbliższym czasie – również opcję VPN (dzięki czemu przekierowywanie ruchu dla dowolnych aplikacji będzie następować bez konieczności uzyskiwania dostępu *root*).
VPN	Podobnie jak w przypadku komputera, użycie VPN na telefonie jest wysoce użyteczne, bo maskuje treść danych – warto wybrać dostawcę usługi VPN, który nie pobiera dodatkowej opłaty za komórkę.
Opcjonalnie: **App Ops** https://play.google.com/store/apps/details?id=com.findsdk.apppermission Aplikacja na Androida	Aplikacja, dzięki której możemy ograniczać uprawnienia do naszych danych wybranym aplikacjom.
Opcjonalnie: **AppLock** https://play.google.com/store/apps/details?id=com.domobile.applock Aplikacja na Androida	Aplikacja umożliwiająca dodatkowe zabezpieczanie wybranych aplikacji hasłem.
Opcjonalnie: **Orfox** https://dev.guardianproject.info/projects/google-summer-of-code/wiki/Orfox_-_Firefox-based_Privacy_Enhanced_Browser/1 Aplikacja na Androida **Onion Browser** https://itunes.apple.com/us/app/onion-browser/id519296448?mt=8 Aplikacja na iOS (płatna 0,99$).	Przeglądarka w wersji beta, kierująca ruch przez sieć Tor, blokująca skrypty i wymuszająca połączenie https, gdy to możliwe. Zdecydowanie polecana, ale ciągle w fazie rozwoju (więc bywają irytujące niedociągnięcia). Dla właścicieli iPhone: Onion Browser.