

Podręcznik cyberbezpieczeństwa dla osób i organizacji aktywistycznych

Kolektyw Rumcajs
Warszawa 2023

Spis treści

Wstęp 3

Rozdział 1 – Bezpieczny Telefon 4

Rozdział 2 – Bezpieczny Komputer 9

Rozdział 3 – Bezpieczny Internet 24

Rozdział 4 – Komunikacja Wewnątrz Grupy 34

Rozdział 5 – Archiwizacja i Usuwanie Informacji 40

Wstęp

Ten podręcznik ma stanowić pomoc w zadbaniu o cyberbezpieczeństwo osób i organizacji aktywistycznych. Korzystając z niego, pamiętaj, że nie jest to podręcznik kompletny. Omawiamy w nim jedynie niektóre najistotniejsze naszym zdaniem zagadnienia. Nie jesteśmy też nieomylni. Choć dołożyliśmy wszelkich starań, by tekst ten nie zawierał żadnych błędów, nie możemy wykluczyć takiej możliwości. Jeśli zauważysz jakiś błąd, będziemy wdzięczni za informację – postaramy się skorygować go najszybciej, jak to będzie możliwe.

Pamiętaj, że nie istnieje coś takiego jak całkowite cyberbezpieczeństwo. Nie istnieją technologie całkowicie nie do złamania. Przy odpowiedniej determinacji i zasobach, wszystko można w jakiś sposób zhakować. Porady, którymi się dzielimy, powodują, że jest to trudniejsze – często wyjątkowo trudne – ale nie ma technologii zapewniającej całkowite bezpieczeństwo zawsze, w każdych okolicznościach.

Wdrażanie mechanizmów bezpieczeństwa

Wiemy, że napisany przez nas tekst jest długi (a i tak jest dopiero wstępem do tematu cyberbezpieczeństwa) i przez to może być przytłaczający. Rozumiemy, że wizja wprowadzenia wszystkich opisywanych przez nas mechanizmów z dnia na dzień może się wydawać niemożliwa. Pamiętaj, że nie musisz robić tego w ten sposób. Dbanie o cyberbezpieczeństwo jest zawsze szacowaniem ryzyka i ocenianiem, która zmiana jest najważniejsza.

Przeglądając nasz podręcznik, wybierz z niego jedno rozwiązanie, wprowadź je i dopiero, gdy poczujesz się z nim komfortowo i nie będzie ono wymagało od ciebie wysiłku, zajmij się wprowadzaniem następnych.

Mamy nadzieję, że tekst ten będzie dla ciebie przydatny. Jeśli masz jakiegokolwiek pytania lub potrzebujesz konsultacji do spraw cyberbezpieczeństwa w twojej organizacji, napisz do nas: kolektyw.rumcajs@protonmail.com

Rozdział 1 – Bezpieczny telefon

Ten rozdział podzielony jest na dwie części. Pierwszą z nich są porady dotyczące zadbania o bezpieczeństwo na twoim prywatnym telefonie. Poruszymy w niej najbardziej podstawowe kwestie dotyczące bezpieczeństwa telefonu, a metody ochrony przed zagrożeniami, które omówimy, będą stosunkowo mało inwazyjne. Część druga będzie dotyczyła telefonów akcyjnych, a więc takich, w których przypadku kwestia bezpieczeństwa powinna odgrywać kluczową rolę. Przedstawimy w niej bardziej zaawansowane rozwiązania związane z ochroną telefonów.

1.1 Telefony prywatne

Aktualizacja

Pierwszą rzeczą, którą należy zrobić w celu zadbania o bezpieczeństwo swojego telefonu, jest jego regularne aktualizowanie. Błędy w systemach operacyjnych są dość częstym zjawiskiem, a większość z nich może posłużyć jako wektor ataku, dlatego niezwykle ważne jest, by twoje urządzenie korzystało z najnowszej wersji systemu operacyjnego, w której błędy z jego poprzednich wersji są już naprawione.

Niestety, producenci telefonów nie mają żadnego interesu w tym, by produkować takie aktualizacje dłużej niż muszą, dlatego większość telefonów traci je po około 3 latach od wypuszczenia danego modelu. Dlatego jeśli zdecydujecie się na wymianę urządzenia, warto jest sprawdzić, jak długo po jego zakupie będzie wspierane aktualizacjami bezpieczeństwa.

Aby zaktualizować telefon należy wejść w: **Ustawienia → System → Aktualizacja systemu**

Blokada ekranu

Porada, by korzystać z jakiejś formy blokady ekranu jest dość oczywista. Niestety odpowiedź na pytanie, jaka forma takiej blokady jest najlepsza, jest już trochę bardziej skomplikowana. Bez wątpienia jednak za dwa najsłabsze rodzaje zabezpieczenia można uznać tak zwanego „wężyka” i odblokowywanie twarzą na telefonach z Androidem (Apple w swoich urządzeniach używa kamery na podczerwień, która jest w stanie zbudować trójwymiarowy obraz twarzy – nie pozwala to odblokować telefonu zdjęciem lub twarzą kogoś podobnego, co jest możliwe w telefonach z Androidem). Tych zabezpieczeń zdecydowanie nie polecamy.

Za najbezpieczniejszą metodę odblokowywania telefonu można uznać długie i skomplikowane alfanumeryczne hasło. Jeśli masz na telefonie dane, na których ochronie bardzo ci zależy, jest to najlepsze rozwiązanie. Niestety, jest ono jednocześnie dosyć niepraktyczne, a że telefon jest urządzeniem, które odblokowujemy najczęściej kilkadziesiąt razy dziennie, zupełnie zrozumiała jest potrzeba, by był to proces szybki i wygodny.

Dwie opcje zapewniające względną wygodę i bezpieczeństwo jednocześnie to kod PIN i odcisk palca lub skan twarzy na urządzeniach Apple. Metody biometryczne mają tę niewątpliwą wadę, że dość łatwo jest za ich pomocą odblokować telefon bez zgody osoby, do której należy dane urządzenie. Z drugiej strony, wpisywany PIN można bez większej trudności podejrzeć (zwłaszcza gdy jest on bardzo prosty, np. 5555, 1212 itp.), a następnie wejść na dane urządzenie nawet bez wiedzy osoby, do której należy dany telefon.

Według nas najrozsądniejszą opcją jest posiadanie co najmniej 6-cyfrowego PIN-u, składającego się z różnych cyfr.

Ochrona przed złośliwym oprogramowaniem

Z powodu technicznej konstrukcji mobilnych systemów operacyjnych, stworzenie skutecznego antywirusa, który byłby z nimi kompatybilny, jest zadaniem niezwykle trudnym, o ile nie niemożliwym. Wszystkie tego rodzaju programy na urządzenia mobilne, o których słyszeliśmy, są wyjątkowo mało skuteczne. Dlatego nie zalecamy instalacji tego rodzaju aplikacji na telefonie. Zamiast tego, dużo lepiej jest dbać o regularne aktualizowanie urządzenia.

Zarządzanie uprawnieniami

W nowszych wersjach Androida i IOS-a, jeśli jakaś aplikacja chce użyć jakiejś funkcji telefonu, musi dostać uprawnienie od osoby, która z niego korzysta. To znaczy, że jeśli chcemy na przykład wysłać zdjęcie za pomocą Signala, to pojawi się nam okienko, czy zgadzamy się na to, żeby Signal uzyskał dostęp do aparatu w telefonie. Jeśli zgodzimy się na to, to aplikacja Signal będzie mogła bez problemu korzystać z aparatu w naszym telefonie, jeśli natomiast nie wyrazimy zgody, to ta aplikacja nie będzie miała możliwości korzystania z aparatu w telefonie. W ramach dbania o prywatność na swoim urządzeniu, warto jest regularnie sprawdzać, jakie aplikacje mają jakie uprawnienia, i dbać o to, by żadna aplikacja nie miała uprawnień, których mieć nie powinna.

Aby sprawdzić, jakie aplikacje mają jakie uprawnienia, należy wejść w: **Ustawienia** →

Prywatność i bezpieczeństwo → **Prywatność** → **Menadżer uprawnień**

Następnie możemy sprawdzić, do czego każda aplikacja ma dostęp i w razie potrzeby jej go odebrać. Niestety, w telefonach z Androidem niektóre aplikacje Google'a są aplikacjami systemowymi i nie ma możliwości odebrania im niektórych uprawnień.

1.2 Telefony akcyjne

W wypadku telefonów akcyjnych kwestia wygody użytkowania jest drugoplanowa, a kluczową kwestią jest ich bezpieczeństwo. Oczywiście w stosunku do telefonów akcyjnych aplikują się wszystkie porady opisane w części pierwszej, warto jednak zabezpieczyć je lepiej.

W tym rozdziale będziemy zajmować się praktycznie wyłącznie kwestiami dotyczącymi telefonów z Androidem. Choć IOS jest systemem stosunkowo bezpiecznym i bardzo dobrze nadającym się do zastosowań prywatnych czy biznesowych, to z perspektywy aktywistycznej nie jest to najlepszy system, z uwagi na bardzo mocne powiązanie urządzenia z kontem osoby, do której urządzenie należy, a także ze względu na małe możliwości konfiguracyjne.

System operacyjny

W tej części opisujemy, w jaki sposób zmienić system operacyjny na urządzeniu. Jeśli nie zdecydujesz się na to (z powodów finansowych lub jakichkolwiek innych) i zostaniesz przy systemie Android, pamiętaj, żeby wykonać twardy (inaczej: fabryczny) reset systemu, jeśli korzystasz z używanego telefonu.

W trakcie pierwszej (lub tej następującej po resecie fabrycznym) konfiguracji telefonu, istnieje możliwość uruchomienia telefonu bez łączenia go z żadnym kontem Google – polecamy tak zrobić. W tym celu należy w każdym możliwym miejscu w trakcie konfiguracji urządzenia kliknąć “Pomiń” i nie wyrażać zgody wszędzie, gdzie będzie to możliwe. Jest to pierwszy krok w zadbanie o anonimowość urządzenia.

Zmiana systemu operacyjnego

Z perspektywy aktywistycznej dwoma podstawowymi problemami z Androidem, jak i IOS-em, jest fakt, że te systemy operacyjne należą do wielkich korporacji, a przy ich projektowaniu priorytetem nie było bezpieczeństwo naszych danych. Dodatkowo obydwa te systemy nie mają otwartego kodu źródłowego, co sprawia, że jako osoby z nich korzystające, nie mamy możliwości kontroli nad tym, co w zasadzie dzieje się z danymi znajdującymi się na urządzeniach. Dlatego jeśli zależy ci na maksymalnym bezpieczeństwie i/lub chcesz przestać korzystać z technologii wielkich korporacji (co w naszej opinii jest jak najbardziej słusznym działaniem), możecie rozważyć zainstalowanie na swoim telefonie alternatywnego systemu operacyjnego.

Pamiętaj jednak, że jest to skomplikowana operacja, a jej niepoprawne wykonanie może zmniejszyć, a nie zwiększyć poziom zabezpieczenia twojego urządzenia. Jeśli potrzebujesz z tym pomocy, albo zastanawiasz się, czy to w ogóle jest ci potrzebne, możesz śmiało do nas pisać.

W tym rozdziale przedstawimy dwa alternatywne systemy operacyjne i dokładnie opiszemy korzystanie z jednego.

/e/OS – to stosunkowo łatwy do zainstalowania i dostępny na wielu urządzeniach system operacyjny o otwartym kodzie źródłowym. Jeśli chcesz usunąć z telefonu oprogramowanie należące do wielkich korporacji i zwiększyć swoją anonimowość, /e/OS może nie być złym wyborem. Jednocześnie warto pamiętać, że priorytetem twórczyn tego oprogramowania nie było zwiększenie prywatności i bezpieczeństwa, ale zbudowanie wygodnego systemu opartego na otwartym kodzie źródłowym i niezależnego od wielkich korporacji. Powoduje to, że /e/OS ma kilka znanych i nienaprawionych problemów z bezpieczeństwem. Dlatego o ile może być on dobrym wyborem na telefonie prywatnym, zdecydowanie odradzamy jego instalację na sprzęcie, który ma służyć do celów aktywistycznych.

GrapheneOS – to bazujący na Androidzie system operacyjny o otwartym kodzie źródłowym, którego głównym celem jest bezpieczeństwo i anonimowość osoby korzystającej z urządzenia. Jako że Graphene bazuje na Androidzie, to jego obsługa jest w zasadzie identyczna, oraz działają na nim te same aplikacje. Jeśli zależy ci na prywatności i bezpieczeństwie, GrapheneOS jest zdecydowanie najlepszym wyborem. Jediną wadą tego systemu jest to, że można zainstalować go jedynie na telefonach Pixel od modelu 4 w górę.

Poradnik do instalacji tego systemu pojawi się w tym miejscu niedługo. W tym momencie polecamy skorzystać z poradnika zamieszczonego na stronie producenta: grapheneos.org/install/web

Alternatywne źródła aplikacji

Jeśli zdecydujesz się na korzystanie z telefonu z Androidem bez konta Google lub z GrapheneOS, nie będziesz mieć możliwości korzystania ze Sklepu Play, a więc tradycyjnej metody pobierania aplikacji na telefon. Dlatego chcielibyśmy wam polecić dwa najlepsze alternatywne repozytoria. Obydwa mają tę zaletę, że, w przeciwieństwie do Sklepu Play, są anonimowe.

F-Droid – to miejsce, z którego wygodnie możemy pobierać aplikacje o otwartym kodzie źródłowym, a więc takie, które z dużą dozą prawdopodobieństwa są stosunkowo bezpieczne. Pobieranie aplikacji nie wymaga zakładania żadnego konta i jest całkowicie anonimowe. Jako że wszystkie dostępne tam aplikacje muszą być na licencji wolnego oprogramowania, to z tego sklepu pobrać możemy raczej prostsze aplikacje, takie jak notatnik czy czytnik PDF-ów, ale za to wszystkie są całkowicie wolne od reklam.

F-Droida można pobrać na tej stronie: f-droid.org

Aurora Store – to rozwiązanie pozwalające na anonimowe pobieranie aplikacji ze Sklepu Play, a więc ze sklepu należącego do Google’a. Jest to najlepszy i najłatwiejszy sposób na pobieranie aplikacji, których nie ma na F-Droid, takich jak Signal.

Sklep Aurora Store można zainstalować, korzystając z F-Droid.

Anonimowe karty SIM

Niestety w tym momencie niemożliwe jest kupienie w Polsce karty SIM tak, żeby nie była powiązana z konkretną osobą. Każdy polski numer jest z kimś powiązany. Dlatego jeśli zależy ci na posiadaniu anonimowego konta na aplikacjach takich jak Signal, które do działania wymagają numeru telefonu, konieczne jest sięgnięcie po niekonwencjonalne rozwiązania. W momencie, w którym piszemy ten podręcznik (listopad 2023), najbliższym krajem, w którym kupić można karty SIM bez rejestracji, są Czechy.

Zakup anonimowych kart SIM

Jeśli chcesz kupić taką kartę SIM, masz dwie opcje:

Allegro – na portalach aukcyjnych jest mnóstwo ofert zakupu czeskich kart SIM. Choć z pewnością jest to opcja najwygodniejsza i wymagająca najmniej wysiłku, to jest ona jednocześnie najmniej bezpieczna, z uwagi na to, że osoba sprzedająca takie karty SIM może połączyć ich numery z danymi osoby kupującej. Dlatego jeśli zdecydujesz się na tę opcję, warto, żeby zakupu dokonała nie osoba, która będzie korzystać z danej karty SIM, ale inna zaufana osoba.

Wycieczka do Czech lub czeska znajoma – zakupienie kart SIM za gotówkę w Czechach jest opcją bezpieczniejszą, ale z oczywistych powodów dużo mniej wygodną.

Jak bezpiecznie używać kart SIM

Każdą kartę SIM zakupioną w Czechach należy aktywować przez internet. Do tego procesu zazwyczaj konieczny jest numer telefonu i karty SIM. Niestety nie możemy przedstawić tutaj instrukcji tego procesu, bo różni się on dla każdego operatora. Jeśli kupujesz karty SIM przez internet, zazwyczaj są one już aktywowane.

Po aktywacji karty SIM, należy włożyć ją do telefonu i aktywować za jej pomocą wszystkie usługi, które chcemy z nią powiązać, takie jak Signal. Następnie należy ją wyjąć z telefonu i zniszczyć, ewentualnie bardzo dobrze ukryć. Do takiego telefonu można następnie włożyć inną kartę SIM lub korzystać z niego łącząc się po Wi-Fi. Dzięki temu nawet jeśli ktoś zabierze nam telefon z ręki, nie będzie dało się połączyć tego urządzenia i/lub karty SIM, która się w nim znajduje, z żadnym kontem w usługach komunikacyjnych.

Rozdział 2 – Bezpieczny komputer

2.1 Podstawowe zagrożenia związane z komputerem

Twój komputer gromadzi wiele informacji o tobie w jednym miejscu. Osoba, która dostałaby hasło do twojego sprzętu, pewnie byłaby w stanie dojść do tego pod jakim adresem mieszkasz, gdzie pracujesz, z jakimi osobami często się spotykasz, w jakich grupach działasz, w jakich akcjach brałeś udział itd. Każda z tych informacji w niepowołanych rękach może stanowić zagrożenie dla ciebie lub osób w twoim otoczeniu.

Dane z komputera mogą zostać wykradzione przy pomocy różnego rodzaju wirusów – niektóre mogą chcieć podglądać cię przy użyciu wbudowanej w laptop kamery, inne będą zapisywać każde twoje kliknięcie w klawiaturę, a jeszcze inne nagrywać ekran. W efekcie narażone mogą być pliki znajdujące się na dysku, ale również hasła do kont internetowych i wiadomości na komunikatorach. W tym rozdziale znajdziesz porady, jak zabezpieczyć swój sprzęt i system operacyjny.

2.2 Pojęcia ogólne

Aktualne oprogramowanie

Wrogie siły nieustannie testują szczelność systemów operacyjnych i programów. Gdy uda im się przełamać zabezpieczenia w danej wersji oprogramowania, wszyscy osoby korzystające z tych wersji są narażone na ataki. Dlatego regularne instalowanie aktualizacji zabezpiecza nas przed znanymi problemami bezpieczeństwa.

Silne hasło

Wraz z postępem techniki rozwinęły się nowe metody zabezpieczania komputerów – skan siatkówki, odcisk kciuka itd. Możemy dzięki nim poczuć się jak w filmie *science fiction* – ale czy te metody są bezpieczne? Co się stanie, jeśli policja nadużyje swoich uprawnień i siłą zmusi cię do przyłożenia palca do czytnika? Zgodnie z polskim prawem nie musisz podawać służbom swoich haseł, stąd są one najbezpieczniejszym sposobem na ograniczenie dostępu do twojego sprzętu. Pamiętaj, żeby były długie – lepsze jest długie hasło bez znaków specjalnych niż krótkie z takimi znakami. Najlepsze będzie oczywiście długie hasło ze znakami specjalnymi. Zapisz je sobie na kartce i trzymaj przy komputerze przez około tydzień. Gdy będziesz mieć już pewność, że je pamiętasz – zniszcz kartkę. Dla ułatwienia możesz utworzyć hasło z jakiegoś zdania, na przykład

„niebieski koń skacze przez krzesło”. Dodaj znaki specjalne – „N1ebl3ski-koń-Skacz3-prz^z-Kr7e\$10” – i bum, masz bezpieczne hasło! Niestety samo hasło do konta na komputerze nie jest wystarczającym zabezpieczeniem, dlatego zaszyfruj swoje dane.

Szyfrowanie dysku

Czy wiesz, że po wyjęciu dysku z komputera można podłączyć go do innej maszyny i bez żadnego problemu odczytać wszystkie pliki na nim zapisane? Szyfrowanie dysku to metoda zabezpieczania danych przed niepożądanym dostępem, która sprawia, że bez znajomości hasła szyfrowania odczytanie zawartości komputera jest praktycznie niemożliwe, przynajmniej na ten moment (piszemy ten podręcznik w listopadzie 2023). W przyszłości spodziewamy się, że komputery kwantowe staną się o wiele bardziej popularne i ich ogromna moc obliczeniowa sprawi, że łamanie dzisiejszych algorytmów szyfrowania stanie się możliwe. Dotyczy to każdego rodzaju szyfrowania – maili, plików, komunikatorów. Istnieje prawdopodobieństwo, że służby, wyczekiwanie na świat komputerów kwantowych, gromadzą nasze zaszyfrowane dane i liczą na to, że za kilka czy kilkanaście lat będą mogły się do nich włamać. Dlatego podkreślamy, że najbezpieczniejsze dane to takie, których już nie ma, a najbezpieczniejsza komunikacja to taka twarzą w twarz, z daleka od elektroniki.

WAŻNE: zanim weźmiesz się za szyfrowanie dysku, zrób backup! Usuń backup, gdy będziesz mieć już pewność, że szyfrowanie poszło po twojej myśli i na pewno pamiętasz dobre hasło do odszyfrowania.

Kopie zapasowe

Jest wiele sposobów na tymczasową lub trwałą utratę komputera i tylko jeden sposób na odzyskanie kluczowych plików – kopie zapasowe. Zrób eksperyment myślowy – za jakimi danymi z twojego komputera byś tęsknił? Jakie są ci niezbędne do działania albo pracy? Zgraj je na zaszyfrowany dysk zewnętrzny lub skorzystajcie z szyfrowanej chmury – na przykład sync.com. Im częściej będziesz robić kopie zapasowe, tym mniej ważnych plików jest narażonych na zniszczenie.

Programy biurowe

Microsoft wydaje sporo pieniędzy na długoterminową strategię uzależniania nas od ich produktów – w szkole najczęściej uczymy się informatyki na komputerach z darmowym Windowsem, do

momentu zakończenia edukacji mamy możliwość pobrania darmowej licencji na Microsoft Office i Windows w różnych wersjach. Na studiach prowadzący demonstrują różne specjalistyczne programy na Windowsach i nie są w stanie pomóc osobom, które korzystają z open-sourcowych systemów. To sprawia, że dla wygody dużo osób decyduje się korzystać z Windowsa i Microsoft Office i przez lata płacić za licencję.

Niezależnie od tego, czy pracujesz na Windowsie, Macu czy Linuxie, możesz wybrać open-sourcowy pakiet biurowy, który podobnie jak pakiet Microsoft pozwala na tworzenie pokazów slajdów, dokumentów tekstowych czy arkuszy kalkulacyjnych. Ten pakiet to LibreOffice – jest całkowicie darmowy i zawiera znakomitą większość funkcji analogicznych programów z pakietu Microsoft Office. Jak to bywa z nowymi programami – przyzwyczajenie się do niego może chwilę zająć, ale polecamy wykonać ten wysiłek z trzech powodów. Po pierwsze oszczędzasz pieniądze, po drugie nie nabijasz kabzy wielkiej korporacji, po trzecie nie narażasz się na inwigilację ze strony programów o zamkniętym kodzie źródłowym.

2.3 Jak zabezpieczyć komputer fizycznie

Myśląc o bezpieczeństwie naszych komputerów, często skupiamy się na zagrożeniach związanych z oprogramowaniem czy naszym ruchem w internecie, mówimy o hasłach i szyfrowaniu. Pamiętajmy jednak, że sprzęt zabezpieczony nawet najlepszym hasłem wcale nie jest bezpieczny, jeśli odchodząc od niego, nie blokujemy ekranu. Dobrą praktyką jest blokowanie komputera zawsze, gdy spuszcza go z oka – niezależnie od tego, czy jesteśmy w domu, czy w kawiarni. Jeśli nasz dysk jest zaszyfrowany, należy pamiętać, że szyfrowanie nie działa w momencie wygaszenia ekranu – żeby zadziałało, należy całkowicie wyłączyć komputer. Dlatego jeśli chcesz zapobiec wyciekowi swoich danych w razie nagłego nalotu służb – niech twoim nawykiem będzie wyłączanie komputera.

Komputery wyposażone są w przynajmniej dwa sprzęty, które mogą zaatakować hakerzy – kamerę i mikrofon. Zauważamy, że dziś już dość popularną praktyką jest zakrywanie kamer w laptopach specjalnymi zaślepkami. Nie kosztują dużo i są wygodne w użyciu. Zdecydowanie polecamy z nich korzystać, jeśli jeszcze tego nie robisz. Pamiętajmy też o mikrofonach – obgadywanie super tajnych planów przy włączonych komputerach to słaby pomysł. Jeśli wymontowanie mikrofonu i podłączanie zewnętrznego urządzenia tylko wtedy, kiedy go potrzebujesz, brzmi jak za dużo zachodu – po prostu nie przynoś komputera na tajne obrady.

Osobom pracującym często w przestrzeniach publicznych (wspólnych biurach, kawiarniach itd.) zalecamy zakupienie filtra prywatyzującego na ekran. Jest to kawałek folii, który umieszczamy na ekranie. Dzięki niemu ekran widoczny jest tylko, gdy siedzimy na wprost niego – osoba zerkająca z ukosa zobaczy jedynie czarny filtr.

Nie wpinaj do komputera nieznanych pendrive'ów – jeśli to możliwe, prześlij dane w inny sposób. Możesz też przeskanować pendrive pod kątem wirusów, zanim otworzysz jego zawartość.

Gdy zagrożenie inwigilacją jest wysokie i zastanawiasz się, czy ktoś majstrował przy twoim komputerze pod twoją nieobecność, przed wyjściem połóż na pokrywie komputera włos lub jakieś okruszki. Zrób zdjęcie wzoru, w jaki się układają. Po powrocie porównaj zastany wzór. Metoda ta działa oczywiście tylko w pomieszczeniach, w których nie ma zwierzaków i przeciągów ;)

2.4 Jak zabezpieczyć komputer z Windows

Aktualne oprogramowanie

Korzystaj tylko ze wspieranych wersji systemu Windows (obecnie są to wersje Windows 10 i Windows 11). Jeśli to możliwe, korzystaj z wersji Pro. Aktualną wersję systemu możesz sprawdzić wybierając: **Start ► Ustawienia ► System ► Informacje**

Upewnij się, że twoja wersja Windowsa jest aktualna, wybierając: **Start ► Ustawienia ► Aktualizacje i zabezpieczenia ► Windows update ► Sprawdź aktualizacje**

Czasami system operacyjny i niektóre programy potrzebują ponownego uruchomienia komputera, żeby zacząć poprawnie działać. Resetuj komputer po pobraniu aktualizacji.

Sprawdź, jakie programy znajdują się na twoim komputerze i usuń te, które są zbędne, wybierając: **Start ► Ustawienia ► Aplikacje ► Wybierz aplikację ► Odinstaluj**

Szyfrowanie komputera

Bitlocker

Włącz szyfrowanie dysku programem Bitlocker, jeśli korzystasz z Windows 10 lub 11 w wersji Pro, Enterprise lub Education. Wybierz: **Start ► Wpisz w polu wyszukiwania: Zarządzanie funkcją BitLocker ► Włącz funkcję Bitlocker**

System zapyta cię, w jaki sposób chcesz zapisać klucz odzyskiwania – to bardzo ważny klucz, który jest jedyną szansą na odzyskanie danych z dysku w razie zapomnienia hasła. Zapisz go w pliku i umieść na zaszyfrowanym pendrive albo wydrukuj i trzymaj w nieoczywistym miejscu z daleka od komputera – znajomość tego klucza może umożliwić włamanie na twój dysk.

Wybierz opcję „Zaszyfruj cały dysk” i uruchom ponownie komputer. W menu „Zarządzanie funkcją Bitlocker” zobaczysz, że dysk C jest w trakcie szyfrowania. Możesz teraz zaszyfrować pozostałe dyski twojego komputera, klikając na nie i wybierając opcję „Włącz funkcję Bitlocker”. W ten sam sposób możesz też zaszyfrować dyski zewnętrzne i pendrive’y.

Veracrypt

Jeśli twoja wersja Windowsa nie wspiera Bitlockera lub nie ufasz korporacji Microsoft w kwestii szyfrowania, zainstaluj program Veracrypt (możesz zostawić domyślne ustawienia): <https://www.veracrypt.fr/en/Home.html>

Veracrypt pozwala zaszyfrować cały dysk lub poszczególne pliki. Żeby zaszyfrować dysk, wybierz: **System ► Szyfruj partycję lub dysk systemowy ► Normalny ► Zaszyfruj cały dysk ► Nie ► Jeden system ► Zostaw domyślne wartości i kliknij ‘Dalej’ ► Wpisz dwukrotnie mocne hasło i kliknij Dalej ► Kręć myszką aż pasek robi się zielony ► Dalej ► Dalej ► Zapisz plik ratunkowy na zabezpieczonym pendrive’ie – będzie potrzebny, jeśli zapomnisz hasła do odszyfrowania dysku ► Zaznacz Pomiń wersyfikację dysku ratunkowego ► Dalej ► Dalej ► Dalej**

Na tym etapie komputer jest przygotowany do zaszyfrowania dysku, ale nic jeszcze nie zostało zaszyfrowane. Sprawdź, czy na pewno pamiętasz jakie hasło do szyfrowania ustawiłeś w poprzednim kroku. Wybierz „Test” i uruchom ponownie komputer. Zamiast ekranu logowania Windowsa zobaczysz czarny ekran i znak zachęty do wpisania hasła. Wpisz hasło i zatwierdź, klikając „Enter”. Jeśli hasło jest nieprawidłowe, kliknij „Escape”. Windows załaduje się ponownie i umożliwi ci ustawienie innego hasła w Veracrypt.

Jeśli masz już pewność, że hasło jest poprawne, wybierz ‘Zaszyfruj’ – Veracrypt zacznie szyfrować twój dysk. W tym czasie możesz normalnie korzystać z komputera, proces szyfrowania zajmuje trochę czasu.

Gdy dysk zostanie zaszyfrowany, wybierz: **Ustawienia ► Konfiguracja wydajności i sterownika**
► Zaznacz Aktywuj szyfrowanie kluczy i haseł przechowywanych w RAM

Następnie wybierz: **Ustawienia ► Preferencje ► Zaznacz Używaj funkcji bezpiecznego pulpitu do wprowadzenia hasła**

Zapora sieciowa (firewall)

Włącz zaporę, wybierając: **Panel sterowania ► Zapora systemu i zabezpieczeń systemu Windows ► Włącz zaporę systemu Windows (dla ustawień domeny, sieci prywatnej i publicznej)**

Antywirus

Pobierz i zainstaluj antywirus, na przykład Avira, AVG lub MalwareBytes:
<https://www.malwarebytes.com/mwb-download>

Wielkość antywirusów ma darmową wersję, która jest wystarczającą ochroną w codziennym użytkowaniu komputera. Pozwól programowi na automatyczne aktualizacje i automatyczne skanowanie systemu. Od czasu do czasu uruchom ręczny skan systemu.

Ustawienia systemowe

Wejdź w: **Ustawienia ► Prywatność**. W tym miejscu możesz odmówić programom dostępu do różnych zasobów twojego systemu. Przejrzyj tę listę i ogranicz dostępy do tych niezbędnych do poprawnego działania programów.

Widoczne rozszerzenia plików

Wirusy zazwyczaj znajdują się w plikach o rozszerzeniu .exe. Jeśli pobierasz z internetu zdjęcie i zamiast rozszerzenia .jpg, .png czy innego znajomego formatu graficznego widzisz rozszerzenie .exe, nie uruchamiaj takiego pliku – to może być wirus. Żeby widzieć rozszerzenia plików w eksploratorze plików, otwórz eksplorator i wybierz kartę „Widok”. Po prawej stronie zaznacz opcję „Rozszerzenia nazw plików”.

2.5 Jak zabezpieczyć komputer z MacOS

Aktualna wersja systemu

Sprawdź, czy twój system jest aktualny – kliknij ikonkę Apple w lewym górnym rogu i wybierz „Ten Mac”. W dniu, gdy piszemy ten poradnik, najnowsza wersja to 14.1.2. Sprawdź na <https://wikipedia.org/wiki/MacOS>, jaka jest aktualna wersja w chwili czytania tego tekstu.

macOS	
	
macOS Sonoma, the latest release of macOS	
Developer	Apple Inc.
Written in	C · C++ ^[1] · Objective-C · Swift ^[2] · assembly language
OS family	Mac · Unix
Working state	Current
Source model	Proprietary (with open source components)
Initial release	March 24, 2001; 22 years ago
Latest release	14.1.2 (23B92 and 23B2091) ^[3] (November 30, 2023; 4 days ago) ^[±]

Jeśli masz starą wersję systemu, kliknij logo Apple, wybierz **Ustawienia systemowe ► Ogólne ► Uaktualnienia**. Włącz opcję 'Uaktualnienia automatyczne'. W okienku poniżej tej opcji powinna znajdować się informacja o tym, co zrobić, by zaktualizować system.

Aktualne wersje aplikacji

Wejdź do App Store, kliknij w Uaktualnienia i zainstaluj wszystkie aktualizacje dostępne dla twoich aplikacji.

Wejdź w Launchpad i usuń wszystkie niepotrzebne aplikacje (pomiń te, które są zainstalowane fabrycznie, usuwa się je trudno i i tak pojawiają się przy kolejnej aktualizacji systemu operacyjnego).

Blokada ekranu

Kliknij w logo Apple ► **Ustawienia systemowe** ► **Ekran blokady**.

Najbezpieczniejszą opcją jest ustawienie komputera tak, by pytał o hasło za każdym razem, gdy włącza wyświetlacz – w ten sposób możesz po prostu wyłączać wyświetlacz, odchodząc od komputera, i nie martwić się o to, że ktoś usiądzie przy twoim sprzęcie i przeczyta twoje maile.

Ustaw '**Wyłączaj wyświetlacz przy zasilaniu z baterii i braku aktywności**' na 2 minuty.

Ustaw '**Wyłączając wyświetlacz przy zasilaniu z sieci i braku aktywności**' na 2 minuty.

Ustaw '**Wymagaj hasła, gdy wygaszacz jest aktywny lub wyświetlacz był wyłączony**' na '**Natychmiast**'

Szyfrowanie dysku

W ustawieniach systemowych wybierz 'Prywatność i ochrona', a następnie 'FileVault'. Żeby włączyć szyfrowanie, kliknij kłódkę w lewym dolnym rogu okna. Wpisz swoje hasło, a następnie kliknij 'Włącz file vault'. Wybierz drugą opcję: 'Stwórz klucz odzyskiwania i nie używaj mojego konta iCloud'. Na ekranie pojawi się klucz odzyskiwania – zapisz go koniecznie w bezpiecznym miejscu. Jeśli komputer zostanie uszkodzony lub zapomnisz hasła do swojego konta, tylko ten klucz będzie w stanie przywrócić twoje dane z dysku!

Zapora sieciowa

Włącz zaporę sieciową, klikając: **Ustawienia systemowe** ► **Sieć** ► **Zapora sieciowa**. Ustaw suwak na pozycję włączoną, a w okienku które się pojawi, ustaw opcje:

- Pobrane aplikacje podpisane przyjmują połączenia przychodzące automatycznie
- Włącz tryb utajony

Jeśli okienko się nie pojawi, otwórz je klikając w przycisk ‘Opcje...’.

Konta gości

Dodatkowe konta na twoim komputerze to potencjalne źródło zagrożenia – szczególnie jeśli są zabezpieczone słabiej niż twoje konto. Wejdź w: **Ustawienia systemowe ► Użytkownicy i grupy**. Upewnij się, że poza twoim kontem na komputerze nie ma włączonych innych kont. W sekcji ‘Automatycznie loguj się jako’ ustaw wartość ‘Wyłączone’.

Antywirus

Rozważ zainstalowanie programu antywirusowego, polecamy na przykład Malwarebytes.com czy Norton. Wykonuj cotygodniowy skan komputera.

Dodatkowe kroki

Rozważ wykonanie wszystkich kroków spisanych na tych listach:

<https://blog.bejarano.io/hardening-macos.html>

<https://github.com/kristovatlas/osx-config-check>

Rozważ zainstalowanie programów takich jak: OverSight, BlockBlock
(<https://objective-see.com/products.html>)

2.6 Jak zabezpieczyć komputer z Linuxem (Ubuntu)

Aktualna wersja systemu

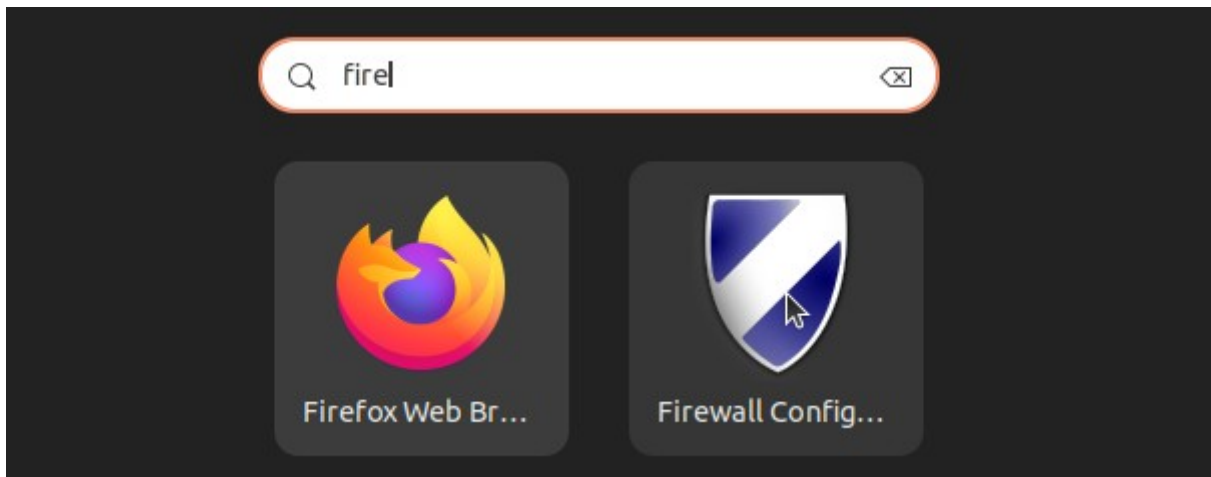
Ubuntu automatycznie informuje o dostępnych aktualizacjach systemu i aplikacji. Nie zwlekaj z ich instalowaniem!

Zapora sieciowa

Zainstaluj program UFW GUI, żeby w wygodny sposób zarządzać regułami blokowania i przepuszczania ruchu sieciowego. Wpisz w terminalu poniższą komendę i kliknij Enter:

```
sudo apt-get install gufw -y
```

Gdy instalacja się zakończy, wyszukaj aplikację w systemie po frazie ‘Firewall’



Po otwarciu aplikacji ustaw pole ‘Status’ na włączony. Od tego momentu twój komputer jest zabezpieczony przed atakami bezpośrednio na twoje porty sieciowe.

Jeśli zauważysz, że aplikacja, która dotychczas działała, po tej operacji przestała – możesz dodać dla niej regułę w programie GFW. Wejdź w zakładkę Reguły i w lewym dolnym rogu okienka programu kliknij przycisk ‘+’, wybierz aplikację z listy aplikacji w ostatnim polu, ustaw politykę ‘Zezwól’ w kierunku ‘Przychodzące’ i zatwierdź klikając ‘Dodaj’.

Jeśli aplikacja nadal nie działa, powtórz poprzedni krok i zamiast kierunku ‘Przychodzące’ ustaw kierunek ‘Wychodzące’. Teraz na liście reguł powinny widnieć dwie reguły, które zezwalają wybranej przez Ciebie aplikacji na komunikację dwustronną przez porty twojego komputera.

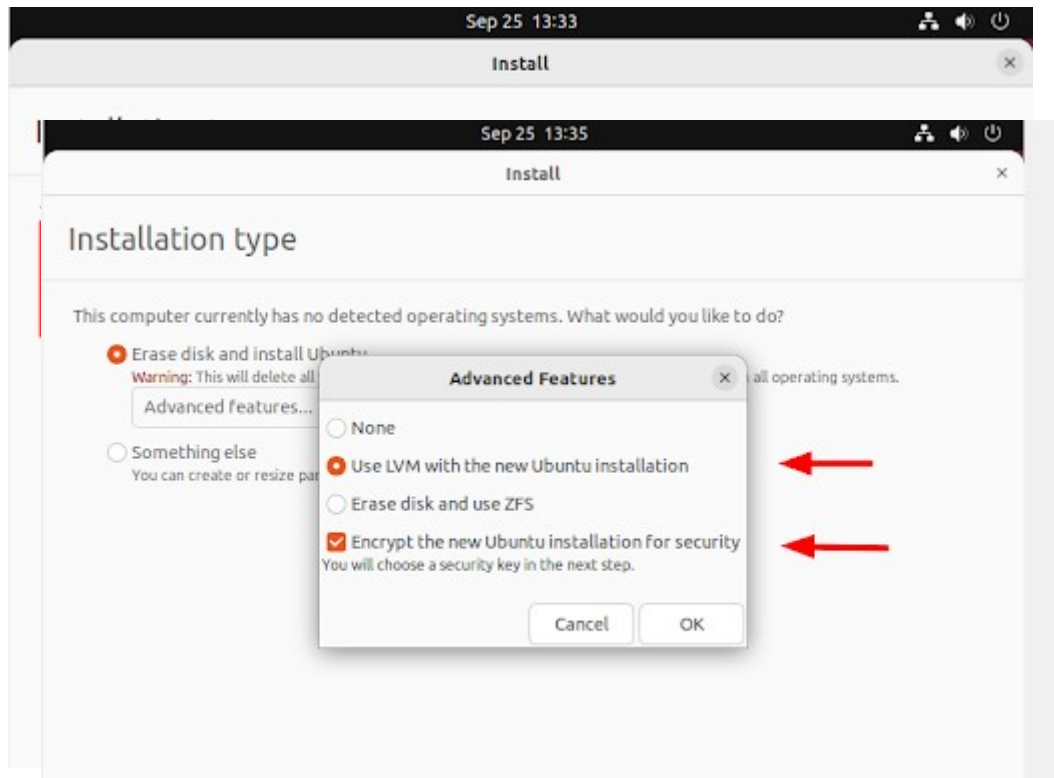
Szyfrowanie dysku

Jeśli korzystasz z niezaszyfrowanego Linuxa, możesz go zaszyfrować tylko przy ponownej instalacji. Nie jest to szybka sprawa, bo trzeba przecież zrobić kopię zapasową wszystkich danych, stworzyć bootowalnego pendrive’a z systemem i zainstalować go od nowa, ale bardzo polecamy ten krok, gdyż znacząco poprawia bezpieczeństwo twojego komputera. Świeży system to też możliwość świeżego startu i nauki nowych, bezpiecznych nawyków w korzystaniu z komputera. Same plusy :)

Żaby zaszyfrować dysk w trakcie instalacji Ubuntu, należy na widoku ‘Installation type’ wybrać pierwszą opcję (Erase disk and install Ubuntu) i kliknąć w przycisk Advanced features.

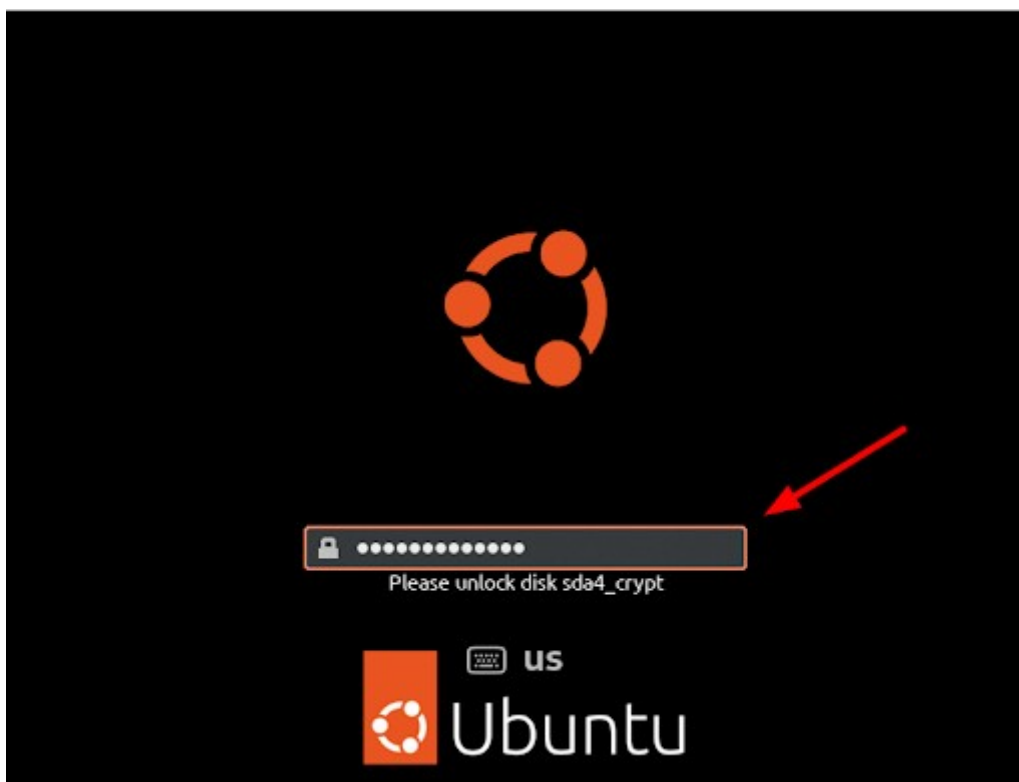
Na okienku które wyskoczy po kliknięciu przycisku zaznacz opcje:

- Use LVM with the new Ubuntu installation
- Encrypt the new Ubuntu installation for security



Następnie kliknij 'Install now' i ustaw bezpieczne hasło zarówno do dysku jak i do pliku z kluczem odzyskiwania (zostanie zapisany w pliku *home/ubuntu/recovery.key*, po instalacji skopiuj go w bezpieczne miejsce – w razie zapomnienia hasła pomoże odzyskać dane z dysku). Kliknij 'Install now' i 'Continue'.

Po poprawnej instalacji uruchom komputer ponownie, zobaczysz następujący ekran:



Podaj hasło do dysku, komputer odszyfruje się i przejdzie do znanego Ci ekranu logowania. Jeśli coś nie wyszło i hasło do dysku nie działa, zainstaluj system ponownie i upewnij się, że nie masz żadnych literówek w hasle podczas jego ustawiania.

Dodatkowe kroki

Osobom bardziej zaawansowanym polecamy ten post do dalszej pracy nad zabezpieczaniem systemu: <https://privsec.dev/posts/linux/desktop-linux-hardening/>

2.7 Tails OS i jak go używać

Tails OS to kompaktowy system operacyjny do zadań specjalnych. Jest dystrybucją Linuxa rozwijaną z myślą o bezpieczeństwie i anonimowości osób z niego korzystających. Tails jest darmowy i, jak wszystkie Linuxy, ma otwarty kod źródłowy. To system przenośny – instalujesz go na pendrive'ie i możesz go uruchomić na dowolnym komputerze. Na maszynie nie zostanie żadna informacja o tym, że działał na niej Tails. Cała komunikacja sieciowa w Tails korzysta z sieci TOR. Więcej o tej sieci dowiesz się w rozdziale 4.

Domyślnie, Tails przy każdym uruchomieniu wygląda jak świeżo zainstalowany system – nie zawiera żadnych plików, ustawień, dodatkowych programów. Zapomina sieci Wi-Fi, do których się łączył, nie pamięta, jaki język był ostatnio używany. Wszystko po to, żeby dać Ci możliwość

wyparcia się zarzutów o korzystanie z tego systemu – „panie władzo, jak niby miałxm prowadzić działalność z tego systemu operacyjnego, jeśli nie ma na nim żadnych plików, historia przeglądarki jest czysta, a lista zapamiętanych sieci Wi-Fi pusta?”.

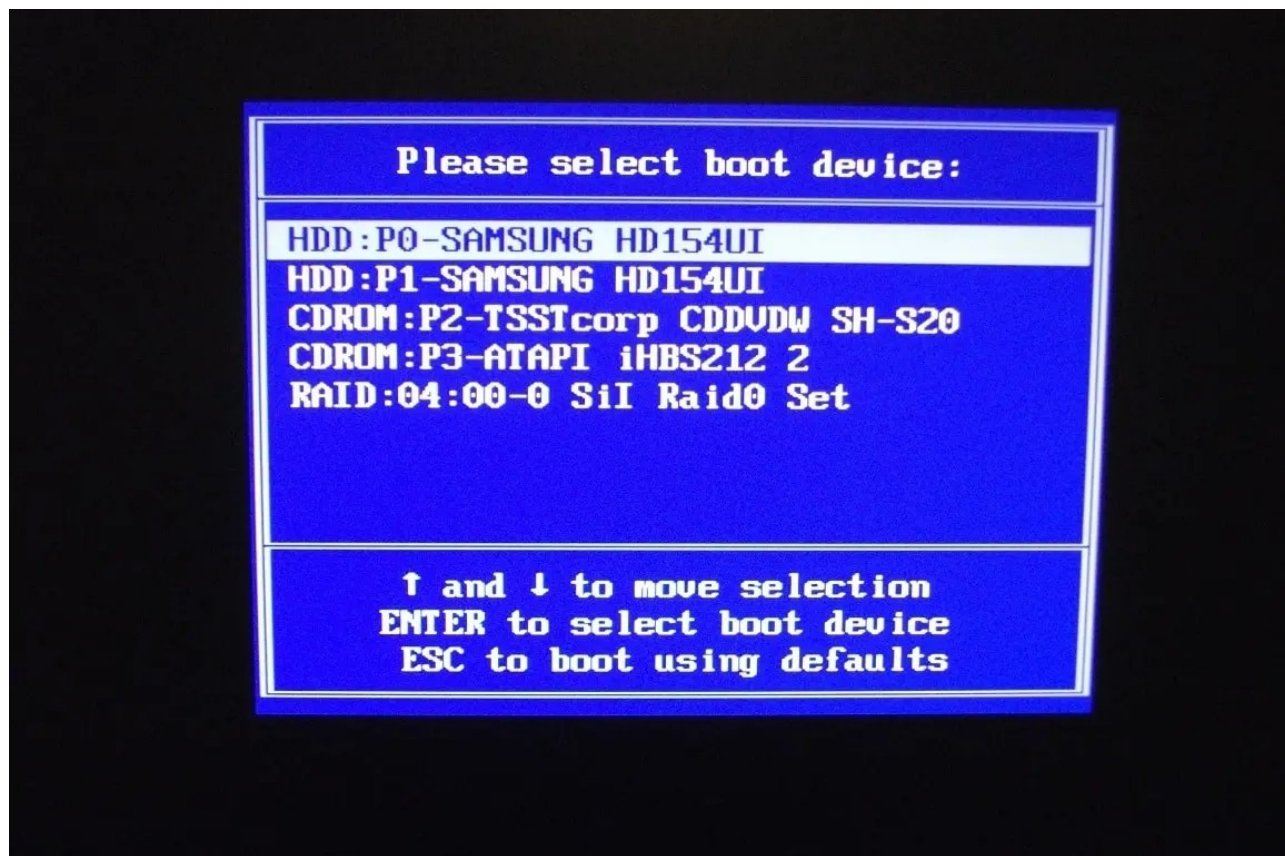
No właśnie, to jak prowadzić na Tailsie jakąkolwiek działalność poza przeglądaniem internetu przez Tor Browser? Przecież czasem trzeba zapisać jakiś plik! No i ile razy można wpisywać hasło do swojego Wi-Fi?! Z pomocą przychodzi mechanizm nazywany 'Persistent Storage' – to zaszyfrowana hasłem część systemu, w której możemy zapisywać swoje ustawienia, zakładki, pliki i połączenia z siecią. Przy uruchomieniu Tails pyta nas, czy chcemy odblokować Persistence. Możemy z tego zrezygnować i uruchomić 'czysty' system, bez śladu naszej obecności. Przydaje się to, jeśli na przykład twoja koleżanka chce wysłać maila. Uruchamiasz Tailsa bez Persistent Storage, twoje pliki są niewidoczne, a ewentualne pliki zapisane przez twoją koleżankę znikną, gdy tylko wyłączysz system. Dość magiczne, prawda? Zobaczmy, jak zainstalować ten cud techniki.

Instrukcje dotyczące instalacji znajdziesz na witrynie tails.net pod tym adresem: <https://tails.net/install/download/index.en.html>. W kroku 1/4 pobierasz obraz Tailsa (jest spory, może to trochę zająć). Następnie możesz wgrać ten plik w pole w kroku 2/4 – witryna sprawdzi, czy plik na pewno jest poprawny i nie został w trakcie pobierania podmieniony przez hakera. W kroku 3/4 przechodzisz do dalszych instrukcji zależnie od systemu operacyjnego, na którym teraz pracujesz. Otwórz ten sam link na telefonie lub innym komputerze, bo w trakcie wykonywania kolejnych kroków trzeba będzie wyłączyć komputer.

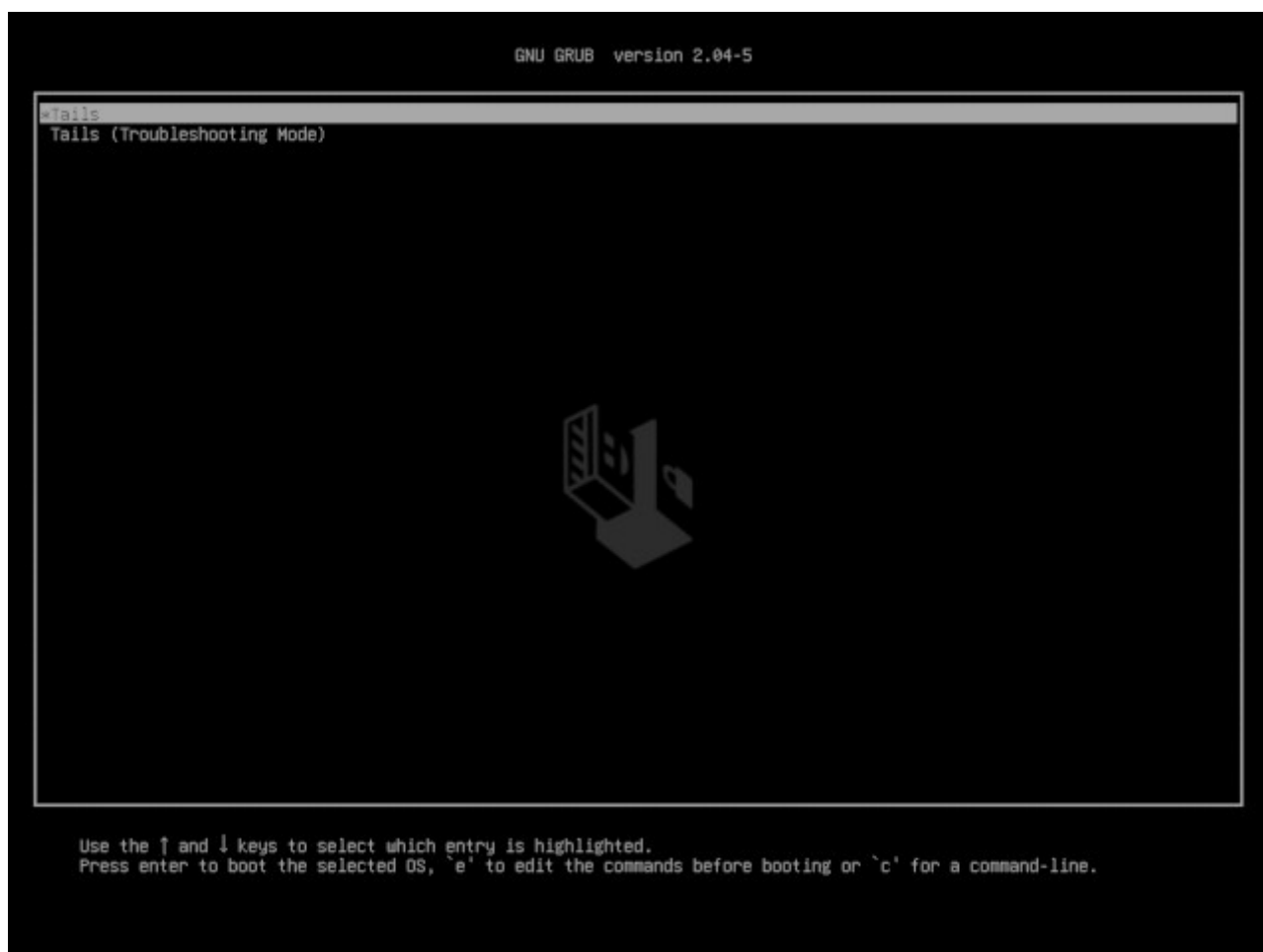
Przygotuj pendrive o pojemności przynajmniej 8 GB. Możesz pominąć pierwsze kroki – masz już pobrany i zweryfikowany obraz Tailsa. W kolejnym kroku stwórz bootowalny pendrive przy użyciu programu rekomendowanego przez instrukcję (Windows i MacOS: balenaEtcher, Linux: GNOME Disks). Otwórz rekomendowany program i podążaj za wskazówkami dla twojego systemu operacyjnego.

Gdy pendrive będzie gotowy, otwórz instrukcję Tailsa na innym urządzeniu, wyłącz komputer, podepnij pendrive i skorzystaj z tabeli na stronie Tailsa, żeby znaleźć klawisz twojego komputera, który uruchamia boot menu. W zależności od producenta i modelu przycisk ten może się różnić – czasem trzeba wypróbować kilka różnych. Żeby wejść do boot menu, uruchom komputer i od razu zacznij naciskać przycisk odczytany z tabelki (np. dla komputera ASUS będzie to ESC, dla Apple –

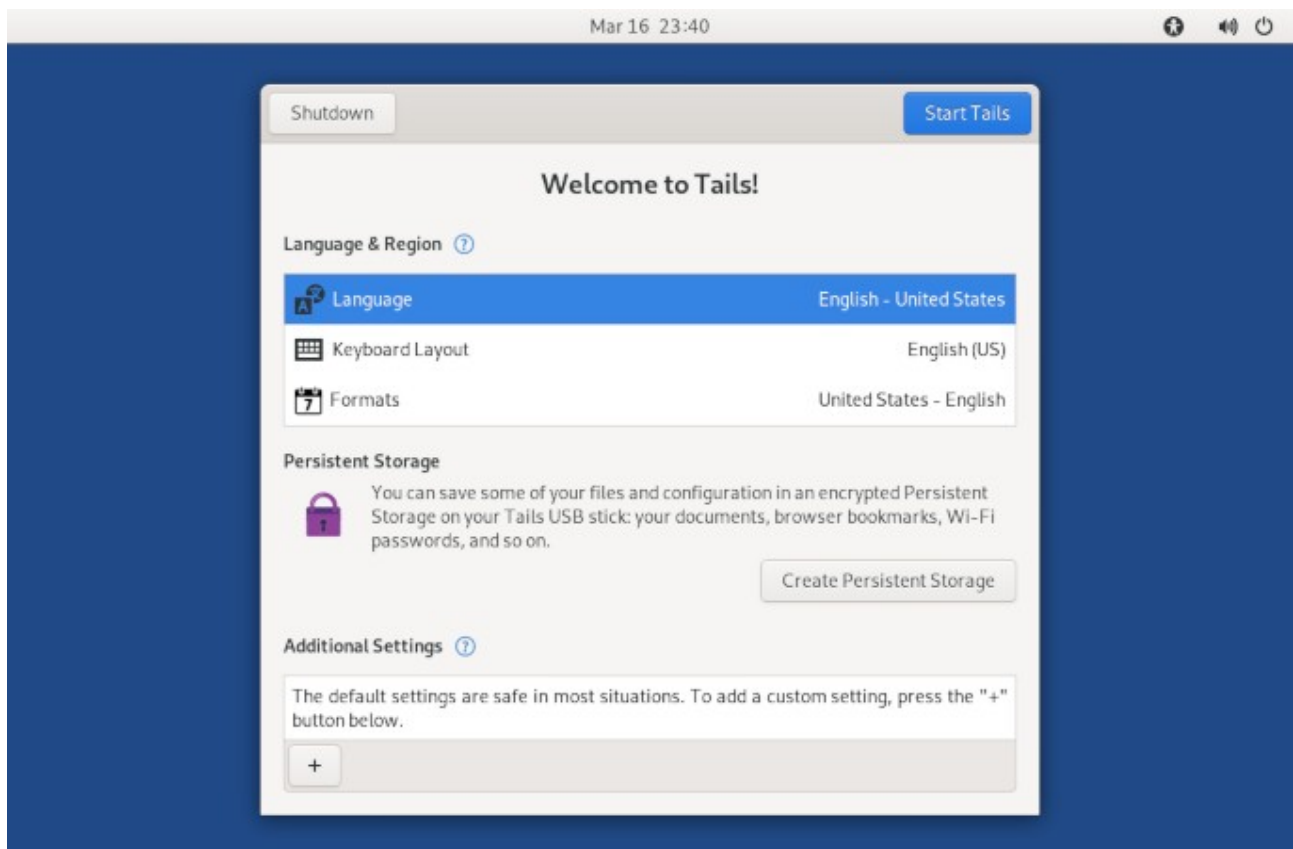
Option). Jeśli komputer uruchamia się tak samo jak zazwyczaj – czyli ładuje twój system operacyjny – wyłącz komputer i spróbuj wciskać inny przycisk.



Gdy uda ci się wejść do boot menu (na każdym komputerze wygląda trochę inaczej) wybierz z listy urządzeń przy pomocy strzałek góra/dół na klawiaturze twój pendrive. W razie problemów z wejściem do boot menu, wyszukaj w internecie frazę „How to enter <marka komputera> boot menu” i zastosuj się do instrukcji.



Jeśli wszystko poszło dobrze, na ekranie pojawi się na kilka sekund ekran z dwoma trybami do wyboru: Tails i Tails (Troubleshooting Mode). Możesz kliknąć ENTER lub poczekać, aż Tails uruchomi się automatycznie.



Gratulacje, masz już Tailsa! Na niebieskim ekranie pojawi się okno ‘Welcome to Tails’, w którym możesz wybrać swój język, układ klawiatury i format daty. Poniżej możesz utworzyć Persistent Storage. Ustaw mocne hasło (w sekcji 3.2 piszemy o tym jak je stworzyć). Gdy Storage będzie gotowy, uruchom Tailsa. Menu znajduje się w lewym górnym rogu. To tam możesz wyszukać dostępne programy i ustawienia. Wybierz *Applications* ► *Tails* ► *Persistent Storage* i wybierz, jakie ustawienia zapisywane są w Storage (wszystkie pozostałe zostaną zapomniane, gdy tylko wyłączysz system).

Informacje o wszystkich funkcjach Tailsa i rozwiązania popularnych problemów znajdziesz w dokumentacji pod adresem: <https://tails.net/doc>

Rozdział 3 – Bezpieczny internet

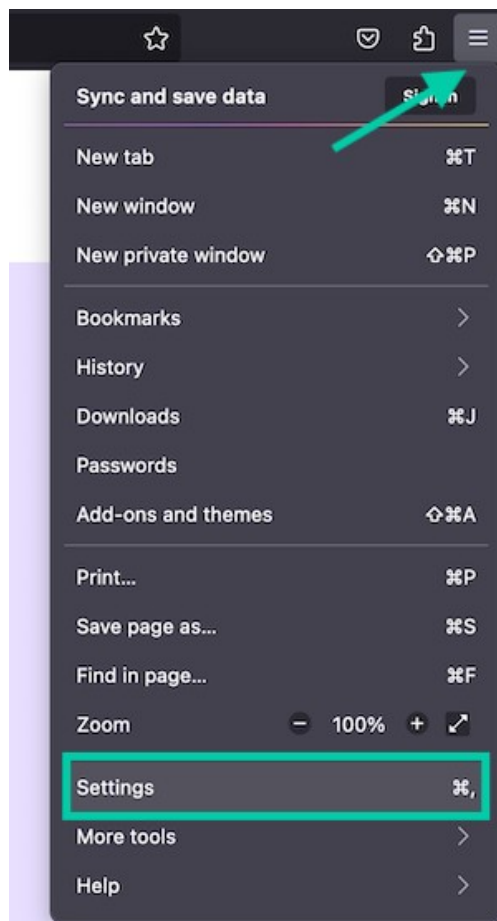
Łączność z internetem jest dziś absolutnie konieczna zarówno do normalnego funkcjonowania, jak i do działania aktywistycznego. W tym rozdziale postaramy się opisać wam najważniejsze zagrożenia związane z łącznością z siecią i podstawowe metody ochrony przed nimi. Skupimy się w nim przede wszystkim na różnych mechanizmach pomagających zachować anonimowość, takich jak VPN i TOR. Napiszemy trochę o tym, z jakich przeglądarek i wyszukiwarek korzystać, oraz opiszemy prawdopodobnie najistotniejsze narzędzie w dbaniu o bezpieczeństwo waszych kont w internecie, czyli menadżer haseł.

3.1 Wybór przeglądarki i jej konfiguracja

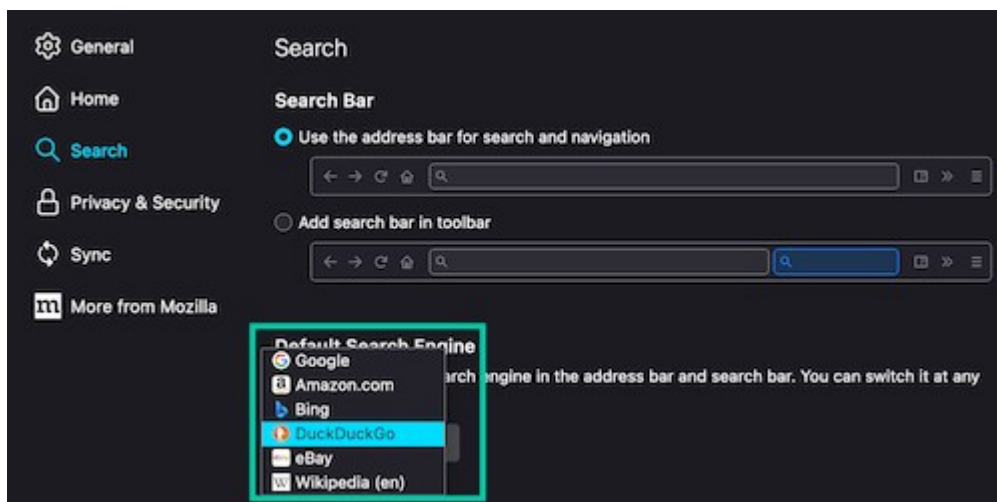
Jako przeglądarkę zdecydowanie najbardziej polecamy wam Firefox. Jest ona jedną z niewielu, które nie są oparte na architekturze stworzonej przez Google'a, oraz należy do fundacji, której model biznesowy nie polega na sprzedaży danych osób korzystających z przeglądarki. Dodatkowo posiada ona bardzo wiele przydatnych funkcji, jeśli chodzi o dbałość o swoją prywatność. Można ją pobrać ze strony mozilla.org.

Jak odpowiednio skonfigurować Firefox

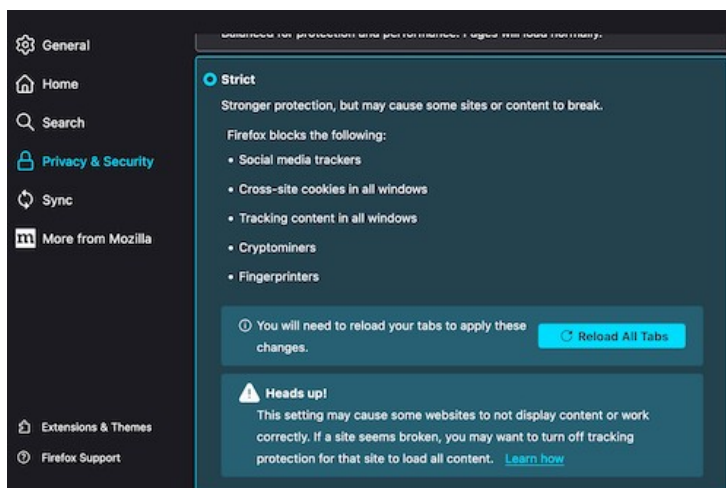
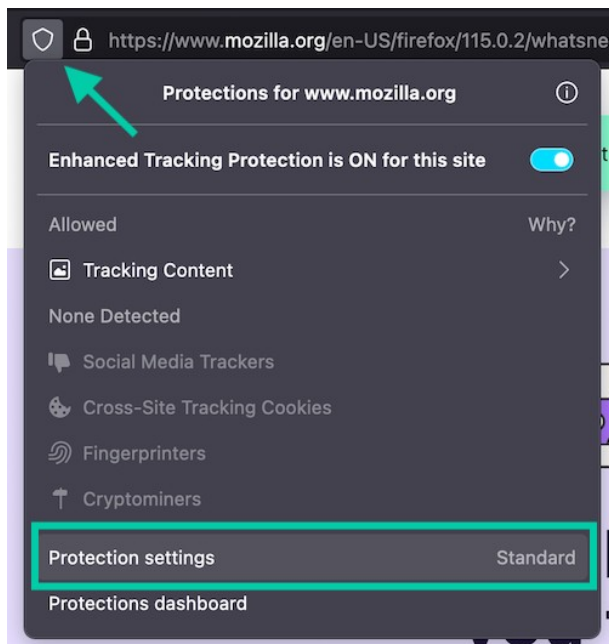
- 1) Po pobraniu i zainstalowaniu przeglądarki, należy zmienić wyszukiwarkę z Google'a na taką, która będzie dbać o naszą prywatność. Według nas najlepszym wyborem jest DuckDuckGo. Aby to zrobić, należy kliknąć w trzy kreski pokazujące się w prawym górnym rogu, a następnie kliknąć Ustawienia.



- 2) Następnie należy kliknąć w opcję Wyszukiwarka, i w okienku “Domyślna wyszukiwarka” wybrać DuckDuckGo.



- 3) Następnie należy ustawić zwiększoną ochronę przed skryptami śledzącymi. Aby to zrobić, należy kliknąć w symbol tarczy w lewym górnym rogu, a następnie w “ustawienia ochrony” i zmienić je na “ściśle”.



Dodatków warto zainstalować wtyczkę do przeglądarki (czyli taki mały program zwiększający możliwości waszej przeglądarki) uBlock (ublockorigin.com), która jest tak zwanym *adblockerem*, czyli zajmuje się blokowaniem reklam i skryptów śledzących na stronach internetowych.

3.2 VPN

VPN, czyli wirtualna sieć prywatna (ang. *virtual private network*), przez agresywne kampanie reklamowe dostawców tego rodzaju usług traktowany jest dziś w popkulturze jako podstawowe i najważniejsze narzędzie pozwalające zadbać o prywatność w sieci. Czy jest tak naprawdę? Trudno powiedzieć, ale raczej nie – choć niewątpliwie mają one swoje zastosowania.

Działanie VPN-a jest w istocie bardzo proste. Tradycyjnie, kiedy łączymy się z internetem, to nasz komputer wysyła prośbę do serwera, a następnie od tego serwera dostaje odpowiedź. Sprawia to, że strony internetowe, z których korzystasz, znają twój adres IP (numer pozwalający na identyfikację),

a administrator sieci Wi-Fi, z której korzystasz, widzi adresy stron internetowych, na które wchodzisz (ma to znaczenie przy korzystaniu z publicznych sieci Wi-Fi). Natomiast kiedy korzystasz z VPN-a, to twój komputer łączy się za pomocą szyfrowanego połączenia z serwerami dostawcy tej usługi i dopiero te serwery łączą się ze stroną docelową. Sprawia to, że adres IP, który dostępny jest dla danej strony internetowej, to adres dostawcy VPN-a, a nie twój prywatny. Dodatkowo, ponieważ ruch pomiędzy twoim urządzeniem a serwerem jest szyfrowany, administrator Wi-Fi, z którego korzystasz, nie widzi, na jakie strony wchodzisz.

Jakie wady ma to rozwiązanie? Korzystanie z VPN-a sprawia, że cały twój ruch internetowy przechodzi przez serwery należące do jednej organizacji. W przypadku, gdy ktoś uzyska dostęp do takich serwerów, będzie miał bardzo dokładną listę wszystkich stron internetowych, z których korzystasz (wiele z największych komercyjnych dostawców VPN-ów ma udokumentowane przypadki współpracy z policją). Warto też pamiętać, że kiedy korzystasz ze stron obsługujących protokół https (czyli w zasadzie wszystkich stron dzisiaj – jeśli jakaś strona tego nie robi, to prawie na pewno twoja przeglądarka cię o tym poinformuje), to co robisz na stronie jest szyfrowanie, a jedyne, do czego ma dostęp administrator Wi-Fi, to sam adres internetowy strony, co nie zawsze jest problemem.

VPN-y, które polecamy

Do użytku prywatnego – Proton VPN i TunnelBear VPN. Obydwa te VPN-y prowadzone są przez stosunkowo godne zaufania firmy, przeprowadzają regularnie niezależne audyty bezpieczeństwa i do tej pory nie miały żadnych dużych wpadek w tym obszarze. Pełna wersja obydwu tych usług jest płatna, ale obydwie mają wersje demonstracyjną. W Protonie polega ona na zmniejszeniu prędkości przesyłu danych i ograniczeniu lokalizacji, z którymi można się łączyć. Darmowa wersja TunnelBear oferuje wszystkie te same funkcje, co płatna, ale ograniczona jest do 2GB przesyłu miesięcznie.

Do użytku aktywistycznego – RiseUp VPN to usługa stworzona specjalnie dla osób aktywistycznych, stworzona przez godną zaufania organizację i polecana przez wiele osób eksperckich. Jest całkowicie darmowa. Największą wadą RiseUp-a jest to, że nie jest on z pewnością najszybszym z VPN-ów, ale o ile nie zamierzasz oglądać za jego pomocą filmów w 4K, nie powinno to być dużym problemem.

3.3 Menadżer haseł

Wyciek danych oznacza sytuację, w której grupa hakerów włamuje się do infrastruktury jakiejś usługi i wykrada z niej dane osób, które z niej korzystają. Najczęściej są to dane logowania, czyli login i hasło. Sytuacja taka jest wyjątkowo niebezpieczna, bo osoba mająca takie dane jest w stanie zalogować się na konta osób, których dane wyciekły, czego skutki mogą być opłakane. Jeśli chcesz

sprawdzić, czy twoje dane zostały udostępnione w jakimś wycieku, można zrobić to na tej stronie: haveibeenpwned.com.

Jeśli tak, należy natychmiast zmienić dane logowania do usługi, z której nastąpił wyciek, oraz do wszystkich innych usług, w których mamy ten sam login i hasło.

Niestety, jako że do wycieków dochodzi nie przez działania ze strony osób korzystających z danej usługi (których dane wyciekają), ale jej dostawcy, nie istnieje w zasadzie żaden sposób, żeby się przed nimi zabezpieczyć. W związku z tym, należy dbać o to, by w razie takiego wycieku, jego skutki nie były dla nas zbyt poważne. Osiągnąć to można przez przestrzeganie następujących zasad:

- 1) Do każdej usługi należy posiadać inne hasło.
- 2) Każde takie hasło powinno spełniać warunki dobrego hasła, czyli być długie (co najmniej 12 znaków), zawierać wielkie i małe litery oraz cyfry i znaki specjalne (np. &, ^, #, }).
- 3) Hasła nie mogą być tworzone według żadnego algorytmu (np. hasło do maila to WHciYB35^MAIL, a do Facebooka WHciYB35^FACEBOOK).

Spełnianie tych trzech warunków gwarantuje, że nawet jeśli nasze dane wyciekną, to nasze hasło będzie trudne do złamania, a nawet jeśli się to uda, to będzie ono umożliwiać logowanie się tylko i wyłącznie do jednego serwisu, a nie wszystkich kont połączonych z loginem.

Niestety, samodzielne spamiętanie tylu odpowiednio skomplikowanych haseł jest w zasadzie niemożliwe, dlatego bardzo polecamy korzystanie z programów, które do tego służą. Takie programy nazywa się menadżerami haseł. Pozwalają one na trzymanie wszystkich danych logowania w jednym zaszyfrowanym pliku. Dzięki temu pamiętać należy tylko jedno hasło (które powinno być bardzo dobre), służące do odblokowania menadżera, w którym znajdują się wszystkie inne dane logowania do naszych kont. Bardzo polecamy wam korzystanie z tego rodzaju oprogramowania.

Wybór menadżera haseł

Menadżer internetowy (mniej bezpieczne):

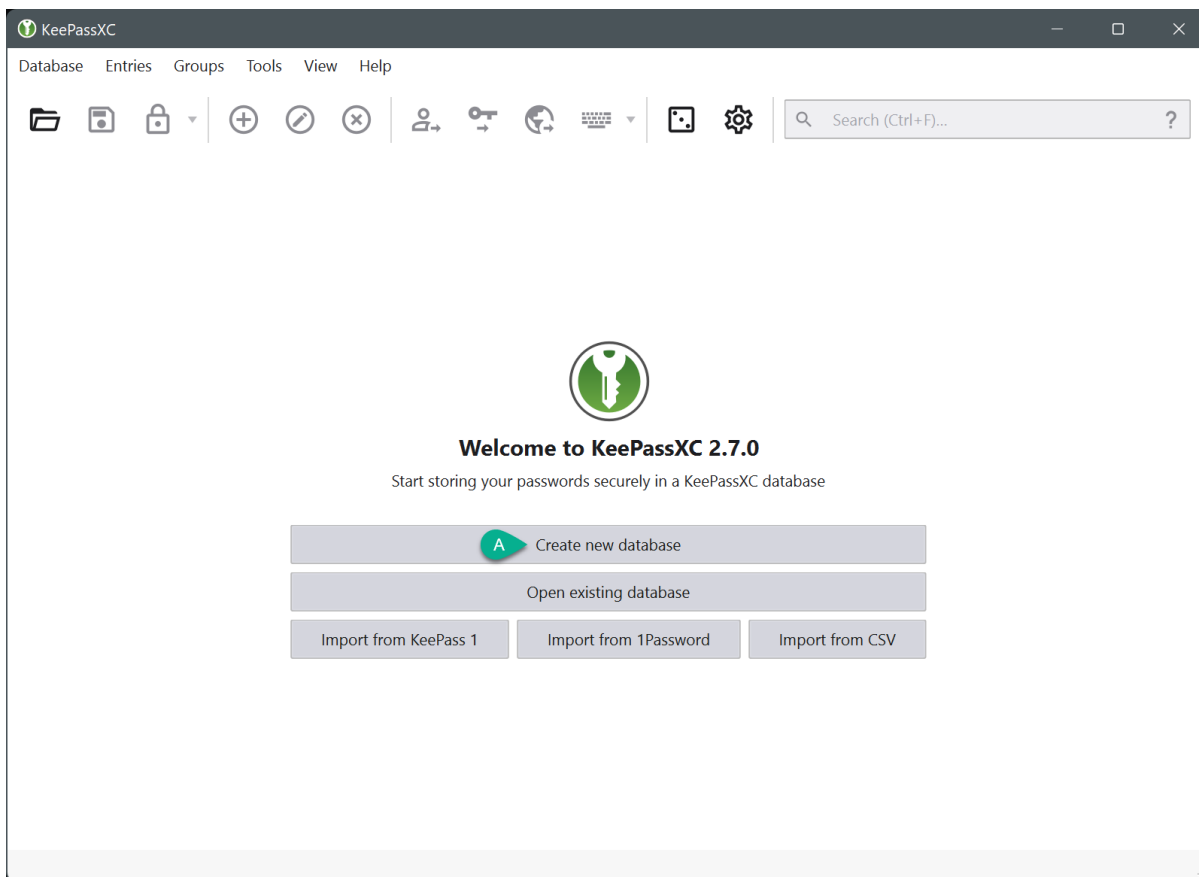
Bitwarden – jeden z najpopularniejszych menadżerów z otwartym kodem źródłowym. Dodatkowo jest całkowicie darmowy. Jego twórcy regularnie publikują raporty bezpieczeństwa. Bitwarden jest polecany przez wiele osób eksperckich zajmujących się bezpieczeństwem.

Menadżer lokalny (najbezpieczniejsze):

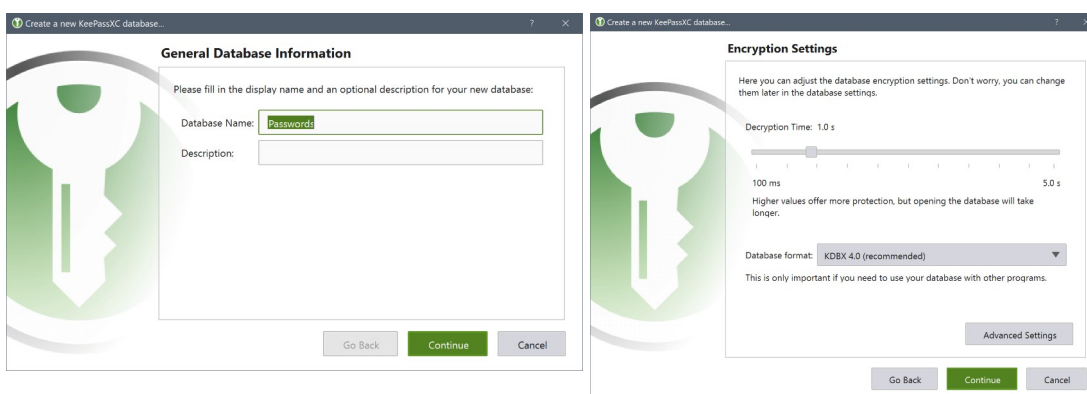
KeePassXC – zdecydowanie najlepszym i najpopularniejszym menadżerem haseł działającym lokalnie (czyli na twoim komputerze, a nie na serwerze należącym do jakiejś firmy), jest KeePassXC. Dodatkowo jest on zupełnie darmowy i ma otwarty kod źródłowy.

Instrukcja konfiguracji KeePassXC

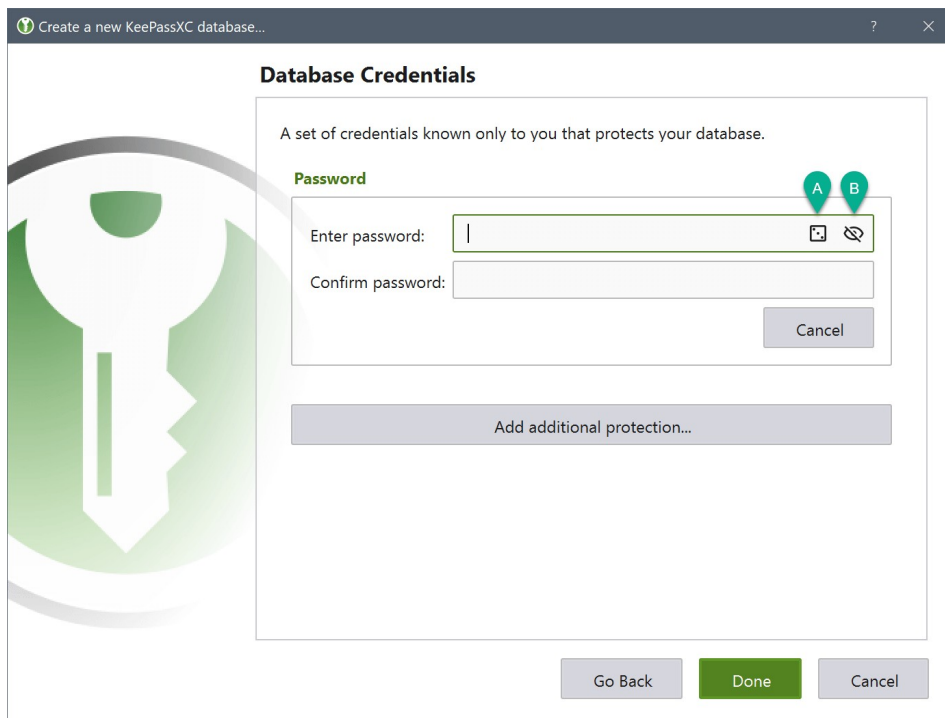
- 1) Aplikację KeePassXC można pobrać z strony internetowej keepassxc.org. Po pobraniu i zainstalowaniu aplikacji otwórz ją, a następnie stwórz nową bazę danych z twoimi hasłami (A)



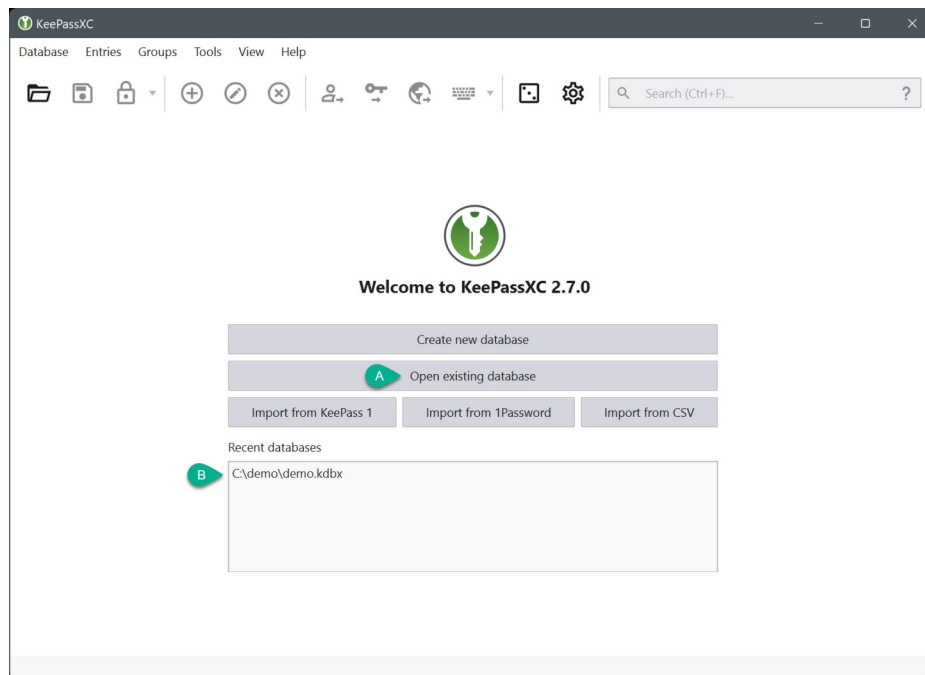
- 2) Ustaw nazwę i opcjonalny opis bazy danych z hasłami, a następnie kliknij kontynuuj, w następnym oknie nic nie zmieniaj i również kliknij kontynuuj.



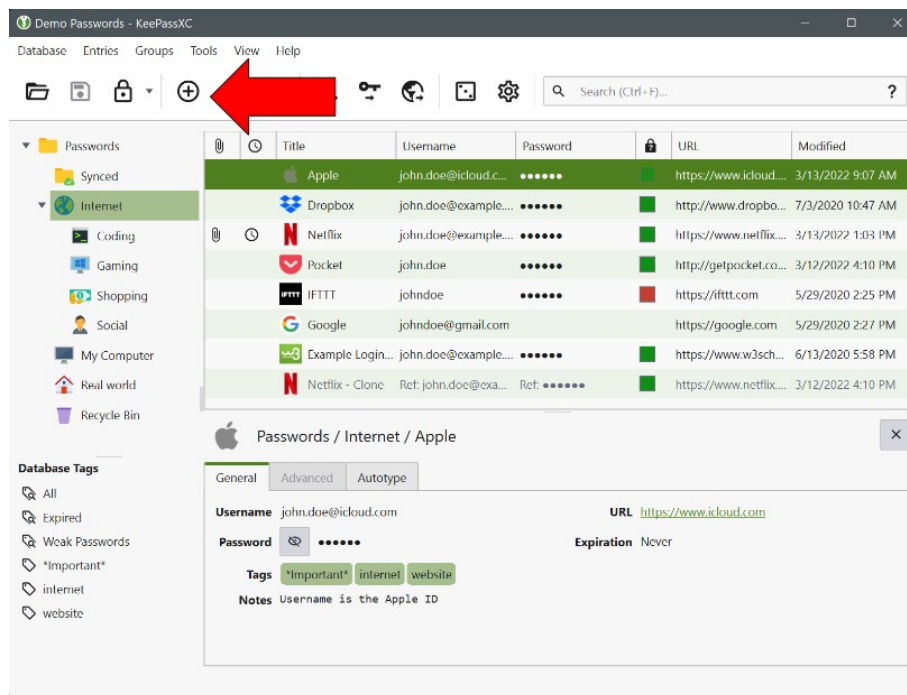
- 3) Następnie ustaw hasło służące do odblokowania tej bazy danych. Pamiętaj, że to bardzo ważne hasło, więc powinno być długie, zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Niestety, w razie utraty takiego hasła nie ma możliwości odzyskania go, dlatego trzeba je bardzo dobrze zapamiętać. Po potwierdzeniu hasła, należy kontynuować.



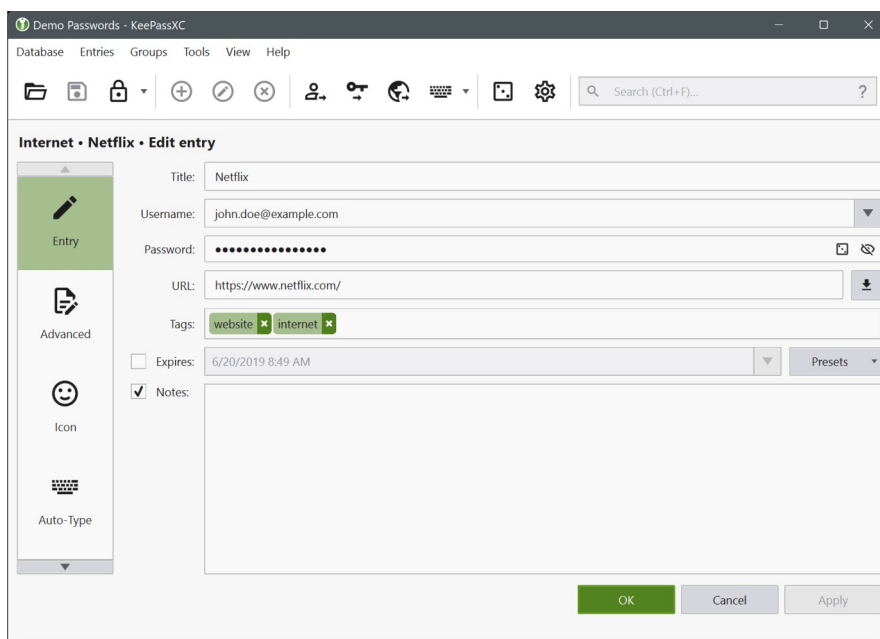
- 4) Po tym kroku na twoim pulpicie zapisany zostanie plik, którego nazwa będzie taka sama jak nazwa bazy danych wybranej przez ciebie w punkcie 2. Plik ten będzie posiadał rozszerzenie .kdbx. To w nim zapisane będą wszystkie twoje hasła. Pamiętaj, aby regularnie robić jego kopię zapasową. Jeśli go utracisz, stracisz dostęp do wszystkich zapisanych danych.
- 5) Aby wejść do utworzonej bazy danych, należy wybrać opcję “otworzenia istniejącej bazy danych” (A), następnie wybrać odpowiedni plik (B) i kliknąć kontynuuj.



- 6) Po odblokowaniu bazy danych mamy możliwość korzystania z zawartych w niej zasobów. Żeby wprowadzić dane logowania, kliknij duży znak +.



- 7) Następnie należy wprowadzić dane logowania, które chcemy trzymać w KeePassXC, wraz z opcjonalnymi informacjami, takimi jak tagi czy adres internetowy danego portalu. Dodatkowo kliknięcie ikony kostki w polu służącym do wpisywania hasła pozwoli na losowe wygenerowanie silnego hasła. Po kliknięciu OK, wpisane dane zostają zapisane.



- 8) Zaczynaj korzystać z KeePassXC. Jeśli chcesz dowiedzieć się więcej o funkcjach tej aplikacji, na jej stronie znajduje się bardzo obszerny poradnik.

Jak korzystać z menadżera haseł

Po wybraniu i skonfigurowaniu menadżera haseł, należy zapisać w nim dane logowania do wszystkich usług. W tym momencie warto zmienić hasła we wszystkich usługach, tak by każde z

nich było unikatowe i mocne. Warto pamiętać, że korzystając z menadżera, nie należy trzymać haseł poza nim.

3.4 TOR

Jeśli zależy ci na maksymalnej anonimowości podczas korzystania z internetu, rozważ korzystanie z TOR-a (ang. *The Onion Router*). W największym skrócie, techniczne działanie TOR-a polega na tym, że ruch sieciowy jest potrójnie szyfrowany, a następnie przechodzi przez trzy niezależne od siebie serwery. Rozproszony charakter i wiele poziomów szyfrowania sprawia, że prześledzenie ruchu w tej sieci jest w zasadzie niemożliwe. Dlatego jeśli potrzebujesz zadbać o pełną anonimowość, jest to najlepsze rozwiązanie.

Jak rozpocząć korzystanie z TOR-a

Korzystanie z sieci TOR należy zacząć od pobrania służącej do tego aplikacji. Znaleźć ją można na stronie TOR Projekt (www.torproject.org). Kiedy już to zrobimy, należy ją uruchomić. Tor Browser automatycznie nie otwiera się w trybie pełnoekranowym, ale w standaryzowanej wielkości oknie. Jest to jeden ze sposobów anonimizacji użytkowników, dlatego o ile to możliwe nie zmieniaj wielkości okna. Po otwarciu aplikacji, należy potwierdzić że chce się połączyć z siecią TOR. Po zrobieniu tego, otwiera się okno przeglądarki – i oto znajdujesz się w owianym złą sławą darknecie. Należy pamiętać, że choć z perspektywy technicznej TOR jest dość imponujący, to nie jest on magią zapewniającą wam bezpieczeństwo zawsze i w każdych okolicznościach. Choć to może oczywisty przykład, to warto go podać. Jeśli korzystając ze swojej prywatnej skrzynki mailowej wysyłasz wiadomość, to nie ma znaczenia czy połączysz z siecią TOR czy nie, bo wiadomość ta i tak podpisana jest twoim adresem mailowym, a więc ciężko mówić tu o jakiejś anonimowości. Dlatego jeśli chcesz posiadać jakieś anonimowe i naprawdę niepowiązane z tobą konta w internecie, pamiętaj, żeby korzystać z nich tylko i wyłącznie za pomocą TOR-a. Pamiętajcie też, że aplikacja Tor Browser nie działa jak większość VPN-ów, które szyfrują cały ruch internetowy z waszego komputera – TOR zabezpiecza tylko i wyłącznie działania odbywające się w tej jednej aplikacji.

Dodatkowo wielość mechanizmów zwiększających anonimowość osób korzystających z TOR-a jest dość upierdliwa i powoduje, że nie wszystkie strony działają z tą przeglądarką poprawnie, a niektórych w ogóle nie da się uruchomić. Dodatkowo konieczność wielokrotnego szyfrowania połączenia i przesyłanie go przez wiele serwerów rozsianych po całym świecie sprawia, że jest to niezwykle wolna przeglądarka.

Jeśli chcesz zacząć swoją przygodę z TOR-em, polecamy ten artykuł, zawierający linki do różnych przydatnych stron w tej sieci: itcontent.eu/aktywne-strony-tor

Rozdział 4 - Komunikacja wewnątrz grupy

W tym rozdziale chcielibyśmy opisać różne metody, których możecie użyć do komunikacji wewnątrz waszej grupy, a więc przede wszystkim komunikatory internetowe i e-maile. Zanim jednak to zrobimy, chcielibyśmy dać jedną uwagę wstępną, która w zasadzie dotyczy każdego rozdziału tego podręcznika: NAPRAWDĘ BEZPIECZNA INFORMACJA TO TAKA, KTÓRA NIE ISTNIEJE. Jeśli macie taką możliwość, to zawsze bezpieczniejszą metodą komunikacji jest powiedzenie sobie czegoś osobiście. Im mniej informacji wymieniacie przez internet, tym bezpieczniejsi jesteście.

4.1 Komunikatory internetowe

Z perspektywy dbania o cyberbezpieczeństwo, wybór komunikatora internetowego dla waszej grupy jest niezwykle istotną decyzją, bo to za jego pomocą przekazywać będziecie większość informacji. Dlatego w tym rozdziale chcielibyśmy opisać, czym należy kierować się przy wyborze komunikatora dla waszej grupy, oraz przedstawić parę polecanych przez nas opcji.

Kryteria wyboru

- 1) Obsługa szyfrowania *end-to-end* – szyfrowanie *end-to-end* (zapisywane czasem jako E2E) można przetłumaczyć na polski jako szyfrowanie od użytkownika/użytkowniczki do użytkownika/użytkowniczki. Powoduje ono, że treść wiadomości odczytać mogą tylko i wyłącznie osoba nadająca i osoba odbierająca daną wiadomość, a nie na przykład dostawca tej metody komunikacji.
- 2) Otwarty kod źródłowy/*open-source* – *open-source* oznacza, że każda osoba może sprawdzić, jak wygląda kod źródłowy aplikacji i czy nie robi ona czegoś niepożądanego. Pozwala to na społeczną weryfikację deklaracji producenta.
- 3) Wiarygodność i pewność – dobrze, jeśli komunikator, z którego zdecydujecie się korzystać, tworzony był przez organizację godną zaufania. Warto sprawdzić, czy osoby go tworzące publikują regularnie raporty bezpieczeństwa i poddają się niezależnym audytom. Dodatkową zaletą będzie, jeśli dana aplikacja tworzona jest przez fundację lub inną niekomercyjną grupę.
- 4) Wygoda korzystania i powszechność – ten punkt mówi chyba sam za siebie. Do niczego nie przyda się wam bezpieczny komunikator, jeśli będzie zbyt skomplikowany, by z niego korzystać, albo będzie tak mało znany, że nie będzie korzystać z niego nikt, z kim chcecie się skomunikować.

Najpopularniejsze sposoby komunikacji, których nie polecamy

- 1) **SMS** – komunikacja za pomocą SMS-ów ma tę niewątpliwą zaletę, że jest bardzo łatwo dostępna, oraz nie wyklucza technologicznie osób nieposiadających smartfona. Jednocześnie, z perspektywy bezpieczeństwa, ma ona bardzo poważne wady. Po pierwsze, numer telefonu jest jednoznacznym identyfikatorem połączonym z imieniem i nazwiskiem, a to sprawia, że w wypadku takiej komunikacji nie ma mowy o jakiegokolwiek anonimowości. Dodatkowo, wiadomości przesyłane za pomocą SMS-ów nie są w żaden sposób zaszyfrowane, co powoduje, że operator sieci komórkowej ma do nich całkowity dostęp – a jako że operatorzy sieci komórkowych są firmami działającymi na terenie Polski, to mają obowiązek udostępniać posiadane przez nich dane (a więc również treść waszych SMS-ów) policji.
- 2) **Facebook Messenger** – tak samo jak w wypadku SMS-ów, Messenger nie obsługuje szyfrowania, co sprawia, że Facebook ma nieograniczony dostęp do wszystkich przesyłanych przez ciebie informacji, co w zasadzie skreśla ten komunikator. Jego jedyną wartą zauważenia zaletą jest to, że do korzystania z niego wystarczy adres e-mail, a nie numer telefonu, co sprawia, że jeśli zależy wam przede wszystkim na ukryciu tożsamości, a nie bezpieczeństwie samej komunikacji, może nie być to najgorsze rozwiązanie.
- 3) **WhatsApp** – WhatsApp jest o tyle ciekawym przypadkiem, że jest to komunikator reklamujący się zaimplementowaniem szyfrowania E2E, co teoretycznie sprawia, że powinien być stosunkowo bezpieczny. Jednocześnie jednak aplikacja ta należy do Facebooka, który na swoim koncie ma wiele naruszeń prywatności, co sprawia, że do wypuszczonego przez nich oprogramowania podchodzić należy z maksymalnie ograniczonym zaufaniem. Dodatkowo, korzystanie z WhatsAppa wymaga podania numeru telefonu, a więc jednoznacznego identyfikatora, co sprawia, że to rozwiązanie zupełnie nie jest anonimowe. Mimo to, przez wbudowane szyfrowanie E2E, WhatsApp jest najlepszym rozwiązaniem z trzech opisanych dotąd w tym podrozdziale.
- 4) **Telegram** – choć Telegram powszechnie uważany jest za jeden z bezpieczniejszych komunikatorów, to ma on pewne problemy, które w naszej opinii uniemożliwiają polecenie go z czystym sercem. Wiadomości wysyłane za jego pomocą są szyfrowane E2E (choć tylko po włączeniu odpowiedniej opcji w ustawieniach i nie w konwersacjach grupowych) oraz nie należy on do wielkiej korporacji, która ma interes w handlu naszymi danymi. Jednocześnie nie jest on aplikacją *open-source*, co uniemożliwia społeczną kontrolę. W tym wypadku jest to niezwykle ważne, ponieważ Telegram nie używa powszechnie znanych i wielokrotnie sprawdzanych metod szyfrowania, ale swojego autorskiego protokołu, a to

zwiększa prawdopodobieństwo, że posiada błędy zmniejszające jego poziom bezpieczeństwa. Dodatkowo, aktywacja konta wymaga numeru telefonu, co zmniejsza poziom anonimowości.

Zaletą Telegrama jest to, że ma on funkcje pozwalające stworzyć z niego proto-medium społecznościowe, co czasami jest bardzo wygodne.

Komunikatory zapewniające niezbędne minimum prywatność i bezpieczeństwa

- 1) **Signal** – Signal jest prawdopodobnie jednym z najlepszych wyborów, jeśli chodzi o prywatną i bezpieczną komunikację. Wszystkie wiadomości w nim przesyłane szyfrowane są E2E. Posiada też wiele opcji pozwalających na skonfigurowanie poziomu zabezpieczeń w zależności od potrzeb (na przykład znikające wiadomości) oraz jest stosunkowo powszechny i łatwy w obsłudze, co sprawia, że łatwo go zaimplementować i nauczyć korzystania z niego nawet osoby bardzo nietechniczne. Najpoważniejszą wadą Signala jest konieczność podania numeru telefonu do korzystania z niego, co sprawia, że identyfikacja osoby, do której należy konto, nie jest szczególnie trudnym zadaniem. Co jest niezwykle ważne, Signal jest programem *open-source*. Dodatkowo, właścicielką Signala jest fundacja, a więc organizacja, której model biznesowy jest znany i nie polega na sprzedaży danych.

Na końcu tego podrozdziału znajdziesz porady, jak skonfigurować Signala, by zwiększyć jego bezpieczeństwo.

Komunikatory dla stawiających przede wszystkim na bezpieczeństwo

- 1) **Session** – Session spełnia wszystkie te same wymogi bezpieczeństwa, co Signal, a więc stosuje szyfrowanie E2E, jest aplikacją *open-source* niezbierającą żadnych metadanych o osobach, które z niej korzystają, oraz jest również prowadzony przez fundację. Elementem, który sprawia, że Session znalazło się wyżej w tym rankingu, jest fakt, że do utworzenia konta aplikacja ta nie wymaga numeru telefonu, ani nawet adresu e-mail. Sprawia to, że pozwala ona na dużo większą anonimowość. Jeśli zależy wam przede wszystkim na prywatności i bezpieczeństwie i jesteście w stanie zaakceptować pewne niewygody, Session jest najlepszą opcją.

Jak skonfigurować Signala

- 1) Znikające wiadomości – ustawienie tej opcji sprawia, że wiadomości w waszych konwersacjach znikają po określonym czasie. Sprawia to, że osoba, która uzyska dostęp do waszego urządzenia, nie będzie mogła przeczytać wszystkich waszych konwersacji, ale jedynie te, które odbyły się bardzo nie dawno. Żeby włączyć tę opcję w konwersacji, należy: kliknąć w nazwę osoby z którą rozmawiacie ► kliknąć w opcję “znikające wiadomości” ► ustawić po jakim czasie mają znikać
Żeby włączyć tę opcję globalnie, w całej aplikacji, należy
Wejść w ustawienia ► kliknąć opcję “Prywatność” ► kliknąć “domyślny czas dla nowych czatów” ► ustawić po jakim czasie mają znikać (pamiętajcie, ta opcja zadziała tylko, jeśli zaczniecie z kimś rozmowę po jej ustawieniu – dla wcześniejszych konwersacji musicie ustawić to ręcznie)
- 2) Numer bezpieczeństwa – to numer, który jest unikatowym identyfikatorem twojego konta na Signalu zainstalowanego na konkretnym urządzeniu. Sprawia to, że jeśli zalogujesz się na swoje konto z innego urządzenia, lub odinstalujesz i ponownie zainstalujesz Signala, to zmieni się twój numer bezpieczeństwa.
- 3) Powiadomienia – automatycznie w powiadomieniach Signala wyświetlana jest treść wiadomości i osoba ją nadająca. Sprawia to, że osoba, która będzie miała wasz telefon w ręku, ma możliwość czytania przesyłanych do was informacji bez odblokowywania telefonu. Dlatego warto skonfigurować powiadomienia tak, by nie wyświetlały tych informacji. Żeby to zrobić, należy
Wejść w ustawienia ► kliknąć opcję “powiadomienia” ► kliknąć opcję “pokaż” ► wybrać jakie informacje mają wyświetlać się w powiadomieniu.
- 4) Blokada aplikacji – ta opcja sprawi, że przed wejściem do aplikacji Signal konieczne będzie podanie hasła do telefonu. Dzięki temu nawet jeśli ktoś przejmie twój odblokowany telefon, nie będzie miał dostępu do prowadzonych na nim rozmów. Żeby ustawić hasło, należy wejść w ustawienia ► kliknąć opcję “Prywatność” ► Włączyć “blokada ekranu” ► opcjonalnie ustawić czas po jakim włączać ma się ta blokada
- 5) Niektóre telefony posiadają opcję tak zwanych “sklonowanych” aplikacji, umożliwiającą posiadanie dwóch niezależnych od siebie wersji tego samego programu. Jeśli zdecydujesz się na takie rozwiązanie, np. dla oddzielnego Signala na numer prywatny i akcyjny, zadbaj o to, by bardziej wrażliwe dane trzymać na “oryginalnej” wersji aplikacji, a nie na jej klonie.

4.2 Skrzynki mailowe

Choć większość komunikacji przebiega dziś raczej za pomocą dedykowanych komunikatorów, a nie maili, to o ich bezpieczeństwo również warto zadbać, zwłaszcza że często są one sposobem komunikacji z osobami nienależącymi do danej grupy.

Kryteria wyboru

Zasadniczo, kryteria wyboru nie różnią się znacząco od tych, które opisaliśmy dla komunikatorów.

Polecane

Poziom podstawowy:

- 1) **Proton Mail** – to aplikacja do obsługi maili skupiona na bezpieczeństwie. Jest polecana przez wiele osób eksperckich w tym temacie. Największą wadą Proton Maila jest to, że jest on własnością firmy, która dość agresywnie promuje płatne wersje tej skrzynki (które przy okazji są bardzo spoko – jeśli macie wystarczający budżet, to zdecydowanie rozważyłbym kupienie Proton Maila)
- 2) **Riseup** – ta skrzynka mailowa stworzona jest z myślą o osobach działających politycznie. Obsługuje szyfrowanie i spełnia wszystkie inne warunki, by być godną zaufania. Niestety do stworzenia konta wymagany jest kod aktywacyjny od innego konta, które istnieje już jakiś czas (jeśli potrzebujecie takiego kodu, napiszcie do nas).

Poziom zaawansowany:

- 3) **Tutanota** – to nowo powstała aplikacja do obsługi maili dla osób skupionych na bezpieczeństwie. Jej największą zaletą jest to, że wiadomości z niej wysyłane pozostają szyfrowane, nawet kiedy wysyłacie je do kogoś, kto nie korzysta z infrastruktury Tutanota. Wadą tego rozwiązania jest to, że żeby przeczytać treść tych wiadomości, konieczne jest zalogowanie się do ich serwisu. To skrzynka polecana dla osób, dla których najważniejsze jest bezpieczeństwo przesyłanych informacji.

4.3 Dyski współdzielone

Dyski współdzielone są kolejnym praktycznie niezbędnym elementem do pracy w dużych grupach. Jednocześnie z uwagi na ilość i rodzaj trzymanych na nich informacji, należy zwracać sporą uwagę na ich odpowiednie zabezpieczenie.

Aktualnie najpopularniejszą przestrzenią tego rodzaju są dyski Google'a. Niestety nie są one w żaden sposób zaszyfrowane, a do tego logując się do nich z prywatnych skrzynek mailowych, nie ma mowy o jakiegokolwiek anonimowości. Dlatego w tym rozdziale chcielibyśmy polecić wam dwie alternatywy.

Polecane dyski współdzielone

Cryptpad – to dysk w swojej konstrukcji bardzo podobny do googlowego, a więc można w nim zarówno tworzyć pliki tekstowe, arkusze obliczeniowe, prezentacje i wiele innych, jak i po prostu przechowywać na nim pliki. W zasadzie każda funkcja dostępna na dysku Google jest dostępna na Cryptpadzie. Niestety, darmowa wersja pozwala wyłącznie na przechowywanie 1GB danych. W wypadku korzystania z Cryptpada, warto pamiętać, że usługa ta nie posiada żadnej opcji odzyskiwania konta po zgubieniu hasła. Jeśli je stracie, wszystkie dane trzymane na dysku zostaną utracone.

Dodatkowo bardzo przydatną opcją jest ustawienie hasła do danego dokumentu. Osoba, która uzyska dostęp linku prowadzącego do konkretnego zasobu, będzie musiała znać również hasło. Żeby włączyć tę opcję, należy zaznaczyć opcję “dodaj hasło” przy tworzeniu nowego dokumentu.

Rozdział 5 – Archiwizacja i usuwanie informacji

5.1 Jak bezpiecznie usuwać pliki i foldery

Pliki zapisywane są na dyskach pod postacią ciągów zer i jedynek. Jeśli na dysku jest wystarczająco dużo miejsca, zera i jedynki reprezentujące dany plik będą znajdować się obok siebie. W przeciwnym wypadku twój system plików podzieli plik na mniejsze fragmenty i zapisze je w różnych miejscach na dysku. Lokalizacje wszystkich fragmentów pliku trzymane są na liście przypisanej do tego pliku. Wyobraź sobie dysk jako ogromną książkę – dane zapisane są w rozdziałach, a żeby dowiedzieć się gdzie znajdują się konkretne informacje, musimy mieć spis treści. Gdy otwierasz plik, system plików patrzy na spis treści i ładuje z dysku odpowiednie ciągi zer i jedynek, które składają się na przykład na obrazek ze śmiesznym kotem.

Żeby usunąć plik zazwyczaj klikamy po prostu ‘Usuń’ albo klawisz DELETE i zapominamy o sprawie. Co się wtedy dzieje? Plik ładuje w Koszu, a żeby go odzyskać, wystarczy kliknąć ‘Przywróć’. Niezbyt bezpieczne, prawda? Kliknij prawym przyciskiem myszy na ikonę kosza i opróżnij go.

Prostym sposobem chroniącym przed atakiem polegającym na przeglądaniu naszego Kosza jest usuwanie plików z pominięciem Kosza. Na Linuxie i Windowsie służy do tego kombinacja klawiszy Shift + Delete, na MacOS Option + Command + Delete. Jest to polecane rozwiązanie, jeśli usuwasz pliki, które nie zawierają bardzo wrażliwych informacji.

Usuwanie plików przez Kosz lub z jego pominięciem niestety nie usuwa pliku w 100%. A nawet nie usuwa go wcale! Przy tym rodzaju usuwania niszczona jest tylko lista fragmentów pliku – same ciągi zer i jedynek składających się na obrazek śmiesznego kota nadal są fizycznie na dysku. Wracając do naszej analogii z książką – rozdziały nadal znajdują się w książce, nie mamy za to spisu treści. Miejsca, w których zapisane są fragmenty „usuniętego” obrazka zostają oznaczone jako gotowe do nadpisania. Zapisanie kolejnego pliku może spowodować, że jego fragment nadpisze część naszego obrazka bezpowrotnie. Dlatego właśnie jeśli przez przypadek stracisz jakiś ważny plik, najlepiej przestań korzystać z komputera i jak najszybciej oddaj go osobie, która potrafi odzyskiwać dane – jest szansa, że fragmenty pliku nie zostały nadpisane przez inny plik i można będzie go przywrócić. Im mniej zapełniony dysk, tym większa szansa na odzyskanie danych.

Co w takim razie zrobić, żeby mieć pewność, że plik jest usunięty na dobre i nawet wprawna hakerka nie będzie w stanie go odzyskać? Poniżej przedstawione są rozwiązania dla każdego z popularnych systemów operacyjnych i typów dysków. Możesz je wykorzystać do trwałego usuwania danych z dysku komputera, pendrive'a czy dysku zewnętrznego. Zanim zaczniesz naukę usuwania, zrób kopię zapasową istotnych danych – pomyłki zdarzają się każdemu!

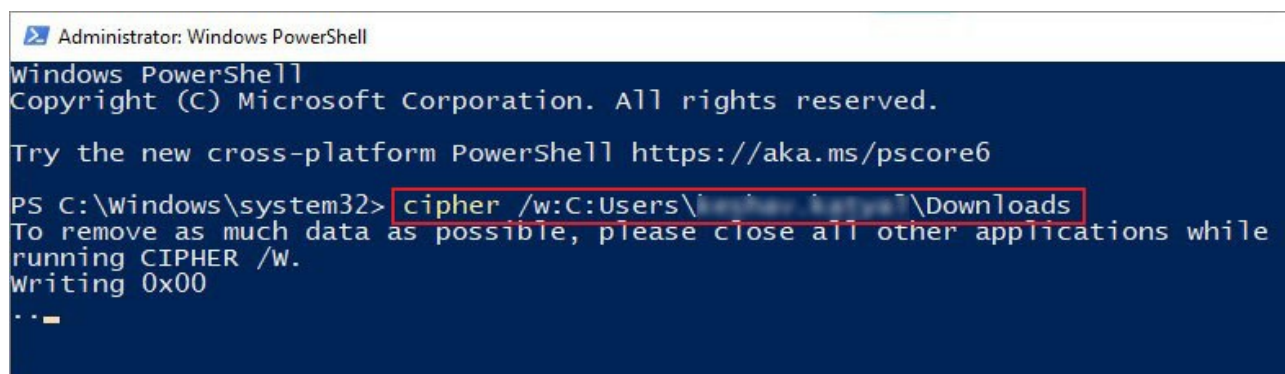
Sprawdź, jakiego typu jest twój dysk:

Windows i MacOS: <https://www.lifewire.com/is-my-storage-ssd-or-hdd-5191369>

Linux (Ubuntu): <https://linuxopsys.com/topics/check-disk-type-ssd-in-linux>

Dysk HDD w systemie Windows

Kliknij Windows + X i wybierz opcję Wiersz poleceń (administrator). Po wpisaniu hasła do twojego konta użytkownika/użytkowniczki, na ekranie powinno pojawić się granatowe okienko:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cipher /w:C:\Users\michal\Downloads
To remove as much data as possible, please close all other applications while
running CIPHER /w.
Writing 0x00
...
```

Żeby bezpiecznie usunąć plik, wpisz komendę **cipher /w:<ścieżka do folderu lub pliku>**. **Zatwierdź ją, klikając ENTER.** Na obrazku powyżej podany jest przykład usuwania folderu **Downloads**. Jeśli chcesz usunąć plik **document.docx** z folderu **Downloads**, komenda będzie wyglądać tak: **cipher /w:C:\Users\<nazwa uzytkownika>\Downloads\document.docx**

Uruchom tę komendę kilka razy – za każdym razem, gdy ją uruchamiasz, w miejsce danego pliku lub folderu na dysku wpisywane są losowe dane. Im więcej razy ją uruchomisz, tym mniejsza szansa na odczytanie nadpisanego pliku. Nie musisz wpisywać komendy za każdym razem od nowa. Wystarczy, że klikniesz strzałkę w górę – wiersz poleceń wybierze wtedy ostatnią wpisaną komendę.

Dysk HDD w systemie Linux (Ubuntu)

Otwórz folder, w którym znajduje się plik do usunięcia. W folderze kliknij prawym przyciskiem myszy i wybierz opcję ‘Otwórz w terminalu’. Pojawi się czarne okienko, wpisz komendę: `shred -zvu -n 5 passwords.list` i zatwierdź enterem.

```
aaronkilik@tecmint ~ $ shred -zvu -n 5 passwords.list
shred: passwords.list: pass 1/6 (random)...
shred: passwords.list: pass 2/6 (ffffff)...
shred: passwords.list: pass 3/6 (random)...
shred: passwords.list: pass 4/6 (000000)...
shred: passwords.list: pass 5/6 (random)...
shred: passwords.list: pass 6/6 (000000)...
shred: passwords.list: removing
shred: passwords.list: renamed to 0000000000000000
shred: 0000000000000000: renamed to 0000000000000000
shred: 0000000000000000: renamed to 0000000000000000
shred: 0000000000000000: renamed to 0000000000000000
shred: 0000000000000000: renamed to 0000000000000000
shred: 000000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: passwords.list: removed
aaronkilik@tecmint ~ $
```

Powyżej podany jest przykład trwałego usuwania pliku o nazwie passwords.list.

Program, który uruchamiamy nazywa się ‘shred’. Przekazujemy mu następujące opcje:

n: ile razy plik powinien być nadpisany (domyślnie 3, w naszym przypadku 5)

z: dodaj jeszcze jedno nadpisanie samymi zerami, żeby ukryć to, że w tym miejscu znajdował się jakiś plik

v: pokaż postęp nadpisywania

u: przytnij i usuń plik po nadpisaniu

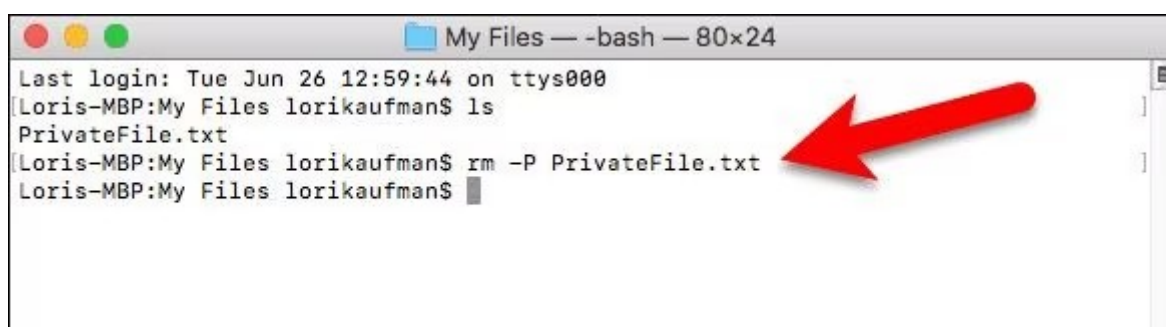
Uruchomienie tej komendy raz wystarczy, żeby trwale usunąć plik. Aby usunąć folder o nazwie `mójFolder` wejdź do niego, kliknij prawy przycisk myszy, wybierz ‘Otwórz w terminalu’ i wykonaj komendę:

```
cd .. && find mojFolder -depth -type f -exec shred -zvu {} \;
```

Komenda składa się z dwóch części: **cd ..** przechodzi do folderu nadrzędnego, a **find mojFolder -depth -type f -exec shred -zvu {} \;** znajduje wszystkie pliki zawarte w folderze mojFolder i jego podfolderach i trwale je usuwa. Zamiast mojFolder wpisz nazwę swojego folderu. Po wykonaniu komendy folder będzie pusty, pozostaje go usunąć, klikając SHIFT+DELETE lub wpisując w linii komend **rm -r mojFolder**

Dysk HDD w systemie MacOS

Otwórz folder zawierający plik do usunięcia, a następnie otwórz terminal wybierając **Finder ► Aplikacje ► Narzędzia ► Terminal**



```
My Files — -bash — 80x24
Last login: Tue Jun 26 12:59:44 on ttys000
Loris-MBP:My Files lorikaufman$ ls
PrivateFile.txt
Loris-MBP:My Files lorikaufman$ rm -P PrivateFile.txt
Loris-MBP:My Files lorikaufman$
```

Pojawi się białe okno linii poleceń. Wpisz w nim komendę **rm**, a następnie chwyć plik do usunięcia i przeciągnij go do terminala. Ścieżka do pliku pojawi się po **rm**. Zatwierdź komendę, klikając ENTER.

W celu bezpiecznego usunięcia folderu dodaj do komendy **rm** opcję **-R**.

Jeśli używasz tych komend pierwszy raz, możesz dla pewności dodać opcję **-i**, która zapyta cię o zgodę na usunięcie każdego pliku. Komendy będą wyglądać więc odpowiednio:

usunięcie pliku: **rm -i <ścieżka do pliku>**

usunięcie folderu: **rm -Ri <ścieżka do folderu>**

Dysk SSD

W przypadku dysków HDD system operacyjny wie dokładnie, w którym miejscu na dysku znajdują się dane. Dyski SSD działają inaczej. Powróćmy znów do analogii z książką. Przy zapisywaniu pliku dysk SSD znajduje rozdział, który nie jest używany, wymazuje go i zapisuje danymi od nowa. Wymazywanie strony niszczy ją jednak odrobinę, więc dysk zarządza zapisywaniem w taki sposób, żeby zrównoważyć wymazywanie poszczególnych rozdziałów i jak najbardziej opóźnić moment, w

którym jakaś strona się przedrze. Wobec tego przy zapisywaniu plików dysk szuka rozdziału, który nie dość, że jest oznaczony jako nieużywany, to jeszcze był wymazywany najmniejszą liczbę razy.

Co więc się stanie, gdy w systemie operacyjnym usuniemy plik i dla pewności spróbujemy go kilka razy nadpisać? Dysk SSD otrzyma informację, że rozdział, w którym był nasz plik, należy oznaczyć jako nieużywany. Następnie kilkakrotnie otrzyma informację, że system chce zapisać kolejne dane (nadpisywanie pliku losowymi danymi). Za każdym razem przejrzy listę wszystkich nieużywanych rozdziałów i wybierze te, które były wymazywane najrzadziej. Nie mamy żadnej pewności, że będzie to ten sam rozdział, który chcieliśmy trwale usunąć.

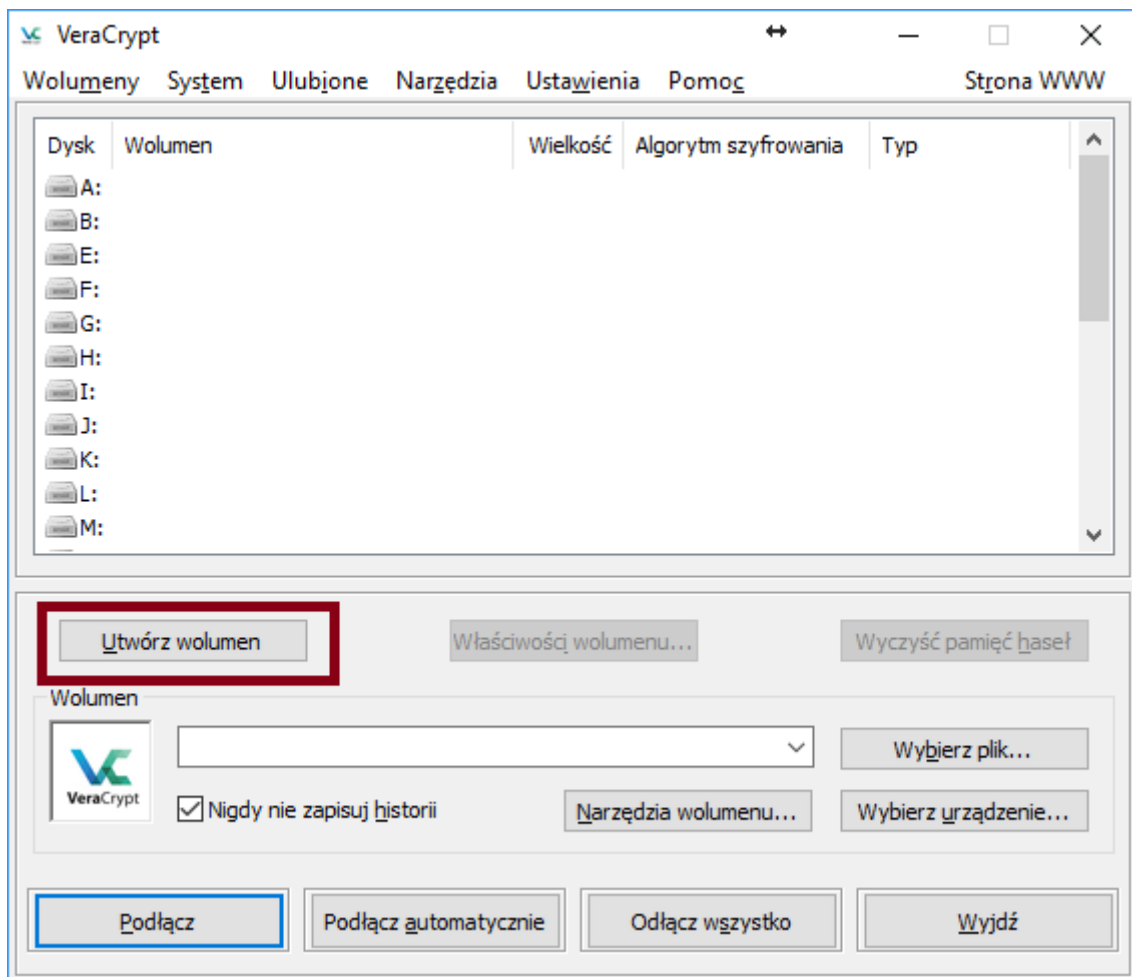
Współczesne systemy operacyjne radzą sobie z tym problemem, uruchamiając co jakiś czas (Windows i MacOS przy każdym SHIFT + DELETE, Linux 18+ raz na tydzień) program TRIM, który ma za zadanie trwale usuwać pliki, które zostały usunięte. Program ten nie gwarantuje jednak 100% skuteczności. Najłatwiejszym sposobem na zabezpieczenie się przed odczytaniem usuniętych plików dysku SSD jest zapisywanie wrażliwych plików tylko w zaszyfrowanych folderach (czytaj niżej) lub zaszyfrowanie całego dysku (opisujemy to w rozdziale 3).

5.3 Szyfrowanie folderów

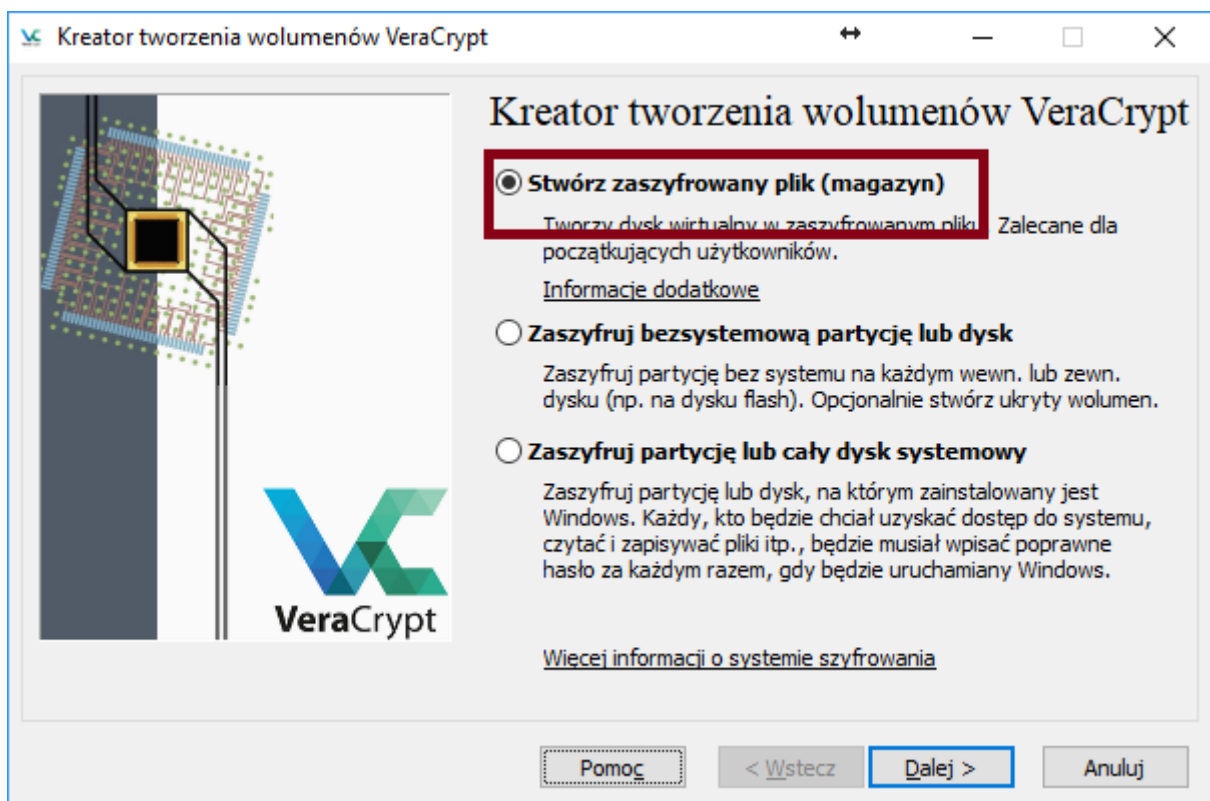
Niezależnie od tego, jakiego systemu operacyjnego używasz, do szyfrowania folderów polecamy program Veracrypt. Pobierz go z tej strony: <https://www.veracrypt.fr/en/Home.html> i zainstaluj (możesz zostawić domyślne ustawienia). Wiele programów typu AdobeAcrobat czy Microsoft Office oferuje opcję zabezpieczania plików hasłem – nie stanowi to dobrego zabezpieczenia przed wprawnym hakerem, dlatego rekomendujemy sprawdzony Veracrypt.

Veracrypt tworzy ‘wolumeny’ – są to pliki, które zachowują się jak foldery (można w nich zapisywać kolejne pliki), a system operacyjny widzi je jako dyski. W uproszczeniu możesz w tym rozdziale rozumieć wolumen jako ‘zaszyfrowany folder’.

Kliknij ‘Utwórz wolumen’

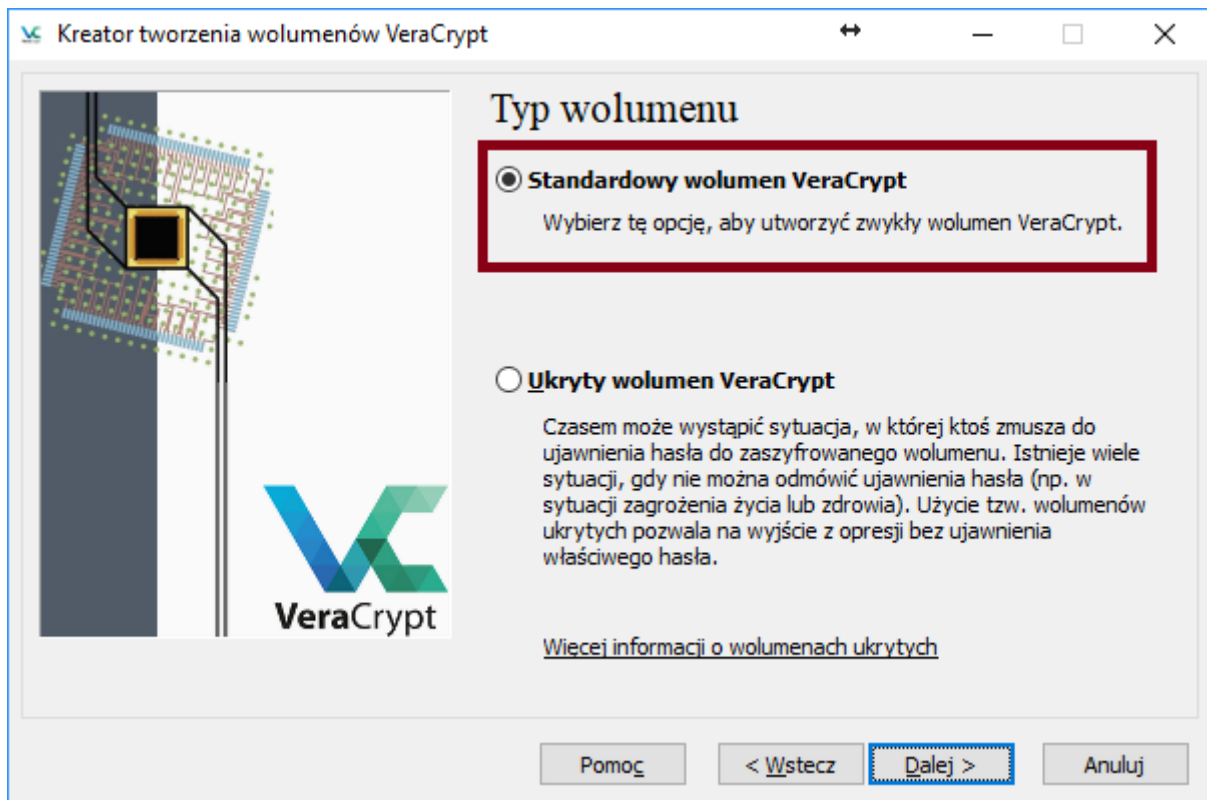


Pozostaw zaznaczoną pierwszą opcję:

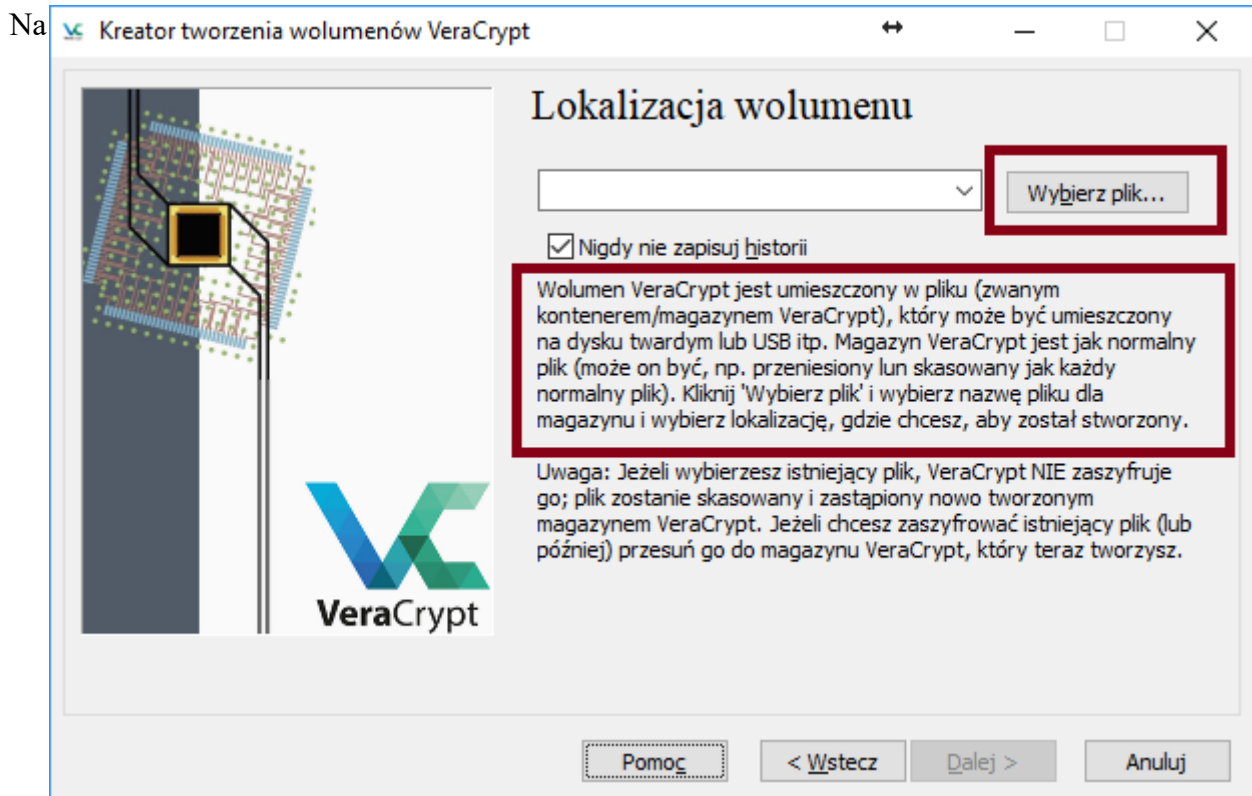


Veracrypt daje nam możliwość stworzenia wolumenu standardowego albo ukrytego. Ukryty wolumen to bardzo ciekawa opcja dla zaawansowanych – pozwala stworzyć wolumen, który ma dwa hasła. Jedno – właściwe – daje dostęp do folderu. Drugie – ‘panic code’ – pokazuje folder z

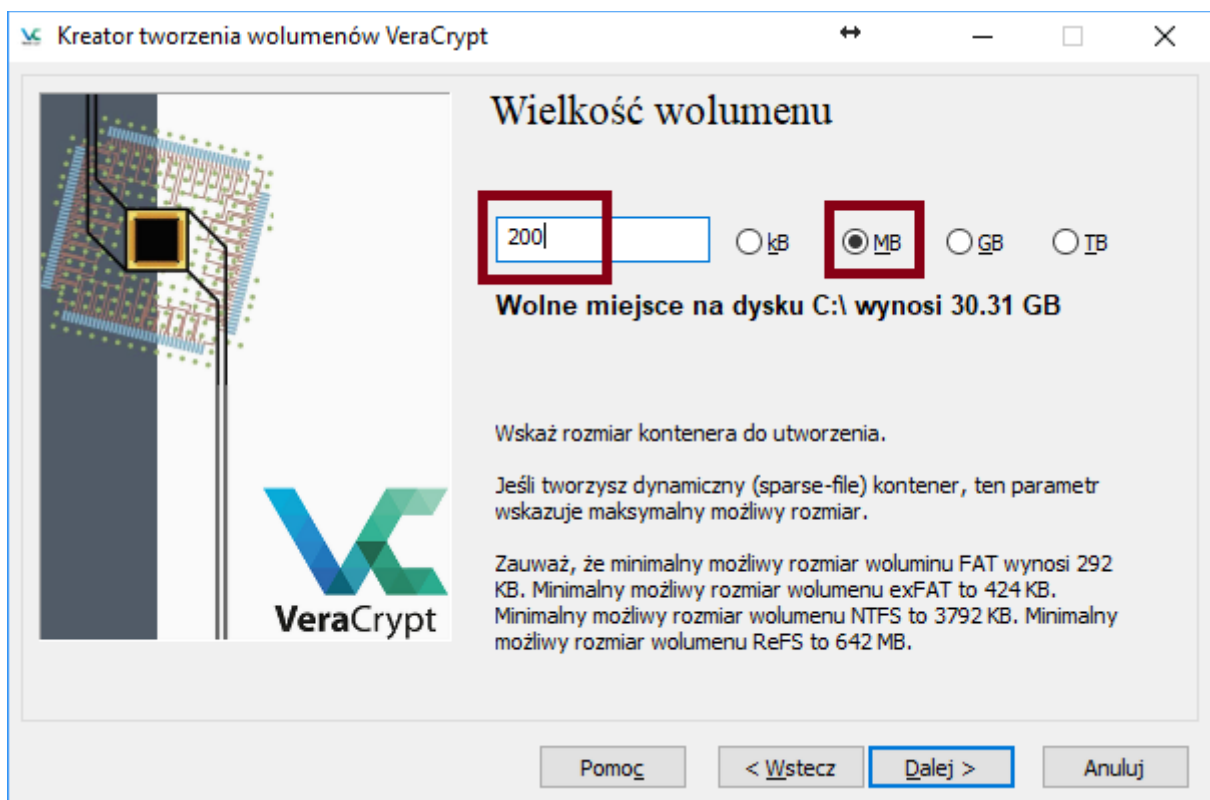
innymi danymi. Tego typu rozwiązanie przydaje się osobom, które obawiają się, że ktoś będzie próbował je zmusić do odszyfrowania wolumenu. Jeśli nie obawiasz się takiego scenariusza, wybierz opcję pierwszą 'Standardowy wolumen VeraCrypt'.



Następnie wybieramy plik, który ma przechowywać nasz wolumen (ważne, żeby nadać mu rozszerzenie '.hc'). Zapisz go w wygodnym miejscu, na przykład na Pulpicie.



następnym ekranie kliknij 'Dalej' i przejdź do ekranu „Wielkość wolumenu”. Wolumen nie powinien być za duży – szyfrowanie i odszyfrowywanie go będzie zajmować za dużo czasu, żeby wygodnie z niego korzystać. Wybierz wielkość adekwatną do Twoich potrzeb:

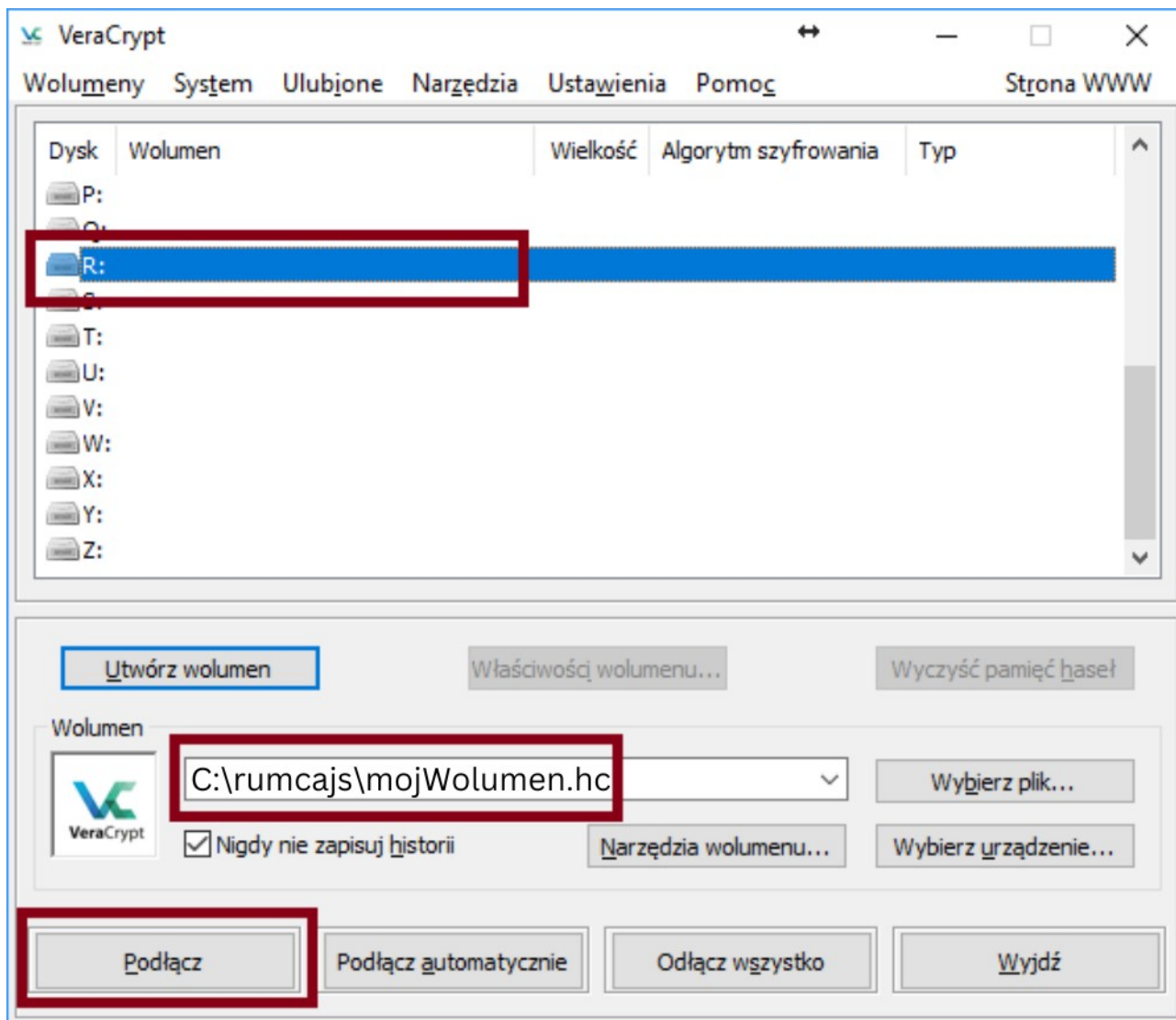


Następnie ustaw mocne hasło (zapisz je na kartce i zniszcz ją dopiero po paru dniach, gdy będziesz mieć 100% pewności, że je pamiętasz – bez niego nie dostaniesz się do danych):

Na

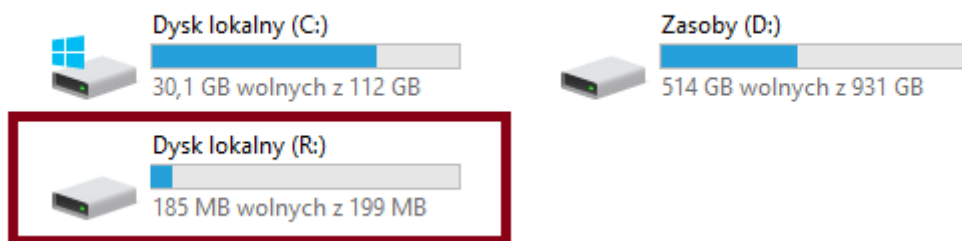
ekranie „Formatowanie wolumenu” wybierz opcję ‘NTFS’ jako system plików (lepiej zarządza przestrzenią na dysku niż FAT). Jeśli korzystasz z MacOS, wybierz opcję FAT. Kręć myszką, żeby pasek na dole ekranu zaświecił się na zielono. Dopiero wtedy kliknij ‘Sformatuj’:

Gdy wolumen zostanie utworzony, możesz zamknąć program Veracrypt. Znajdź teraz plik z rozszerzeniem .hc wybrany przez ciebie jako plik twojego wolumenu. Kliknij w niego dwukrotnie. Program Veracrypt znowu się otworzy i podłączy wolumen, gdy wybierzesz wolną literę, pod jaką ma być podłączony i klikniesz 'Podłącz':



Po wpisaniu hasła, wolumen będzie dostępny jako jeden z twoich dysków. W przypadku Windowsa będzie to wyglądało w ten sposób:

▼ Urządzenia i dyski (3)



Wolumen będzie dostępny tak długo, dopóki nie wyłączysz komputera lub nie klikniesz 'Odłącz' w Veracrypt. Przy ponownym podłączeniu wolumenu, program znowu zapyta o hasło, żeby go odszyfrować.

5.4 Szyfrowanie dysku zewnętrznego

Żeby zaszyfrować dysk zewnętrzny (na przykład dysk, na którym będziesz trzymać kopię zapasową swoich plików albo pendrive), również możesz skorzystać z programu Veracrypt (opisany wyżej).

Wybierz **Wolumeny ► Utwórz nowy wolumen ► Zaszyfruj bezsystemową partycję lub dysk ► Standardowy wolumen Veracrypt ► Wybierz urządzenie...**

Z listy urządzeń wybierz podpięty dysk/pendrive. Jeśli wybrany nośnik jest pusty, wybierz 'Stwórz zaszyfrowany wolumen i sformatuj go', natomiast jeśli na dysku są już jakieś dane których nie chcesz starcić wybierz 'Zaszyfruj partycję w miejscu'. Zostaw domyślny algorytm szyfrowania i algorytm mieszający oraz stwórz hasło do szyfrowania.

Kręć myszką, dopóki pasek postępu nie zaświeci się na zielono, następnie kliknij '**Dalej**'. Kliknij '**Dalej**' i '**Zaszyfruj**'.

Gdy po kilku – kilkunastu minutach szyfrowanie się zakończy, możemy otworzyć nasz dysk. Najpierw odłącz go od komputera i podłącz ponownie. Otwórz menadżera plików twojego systemu. Na liście dysków po lewej stronie okna powinien być widoczny twój dysk. Kliknij na niego dwukrotnie i wpisz hasło odszyfrowywania – jeśli hasło jest poprawne, wyświetli się zawartość dysku. Masz teraz szyfrowany dysk zewnętrzny, który możesz otworzyć na dowolnej maszynie pod warunkiem, że masz hasło do odszyfrowania.

5.5 Jak bezpiecznie czyścić dyski

Sprzedajesz swój dysk zewnętrzny? Chcesz trwale i bezpiecznie usunąć jego zawartość? Wykonaj dwa kroki: zaszyfruj dysk (zgodnie z instrukcją zawartą w punkcie 7.4), a następnie sformatuj go. Proces formatowania polega na czyszczeniu zawartości dysku, coś jak przywracanie dysku do ustawień fabrycznych. Formatowanie wygląda różnie w zależności od systemu operacyjnego, na jakim pracujesz.

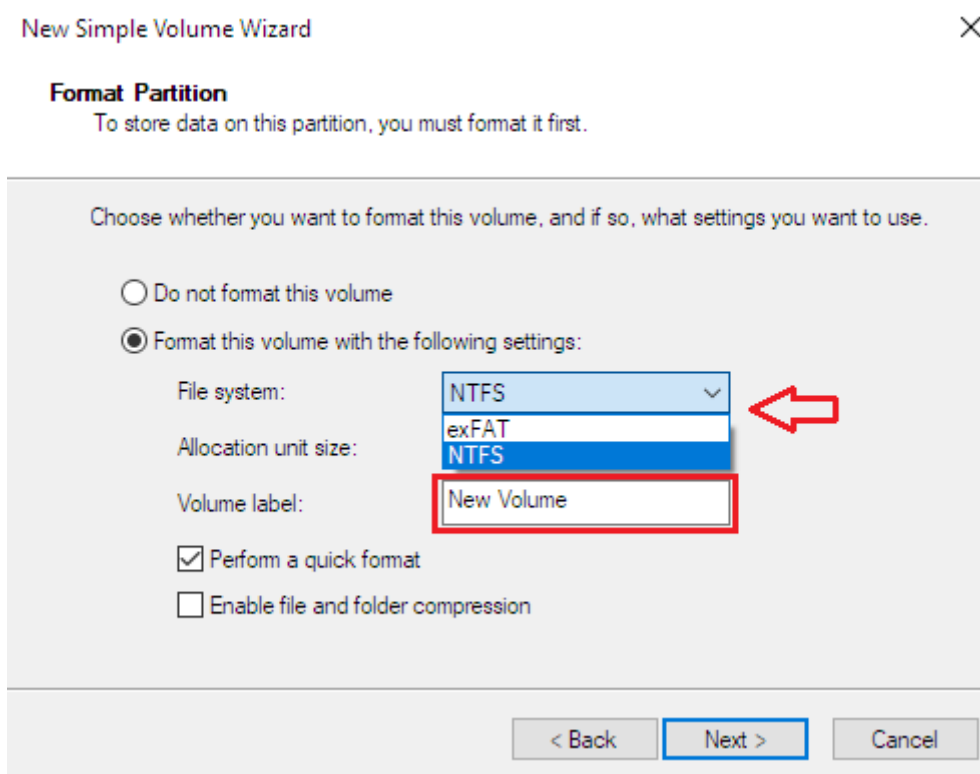
Windows

Otwórz narzędzie zarządzania dyskami klikając **Windows + R** i w okienku uruchamiania wpisując **diskmgmt.msc** oraz klikając **OK**. Jeśli pojawi się prośba o podanie hasła administratora, wpisz je. Zobaczysz listę dysków podłączonych w tym momencie do komputera. Żeby mieć pewność, że czyścisz odpowiedni dysk, możesz odłączyć dysk zewnętrzny od komputera i sprawdzić, który dysk zniknął z listy – ten dysk nas interesuje.

Kliknij na dysk prawym przyciskiem myszy i wybierz opcję **Initialize Disk (Zainicjuj dysk)**. Wybierz rodzaj partycji – MBR dla dysków poniżej 2 TB, GPT dla dysków powyżej tego rozmiaru. Kliknij **OK**, dysk powinien być oznaczony jako Unallocated (Nieprzydzielony).

Kliknij prawym przyciskiem myszy na napis **‘Unallocated’** i wybierz opcję **New simple volume (Nowy prosty wolumen)**. Klikaj **‘Next (Dalej)’** dopóki nie dojdiesz do widoku wyboru systemu plików. Jeśli chcesz używać dysku zarówno na komputerach z MacOS jak i innych, wybierz opcję exFAT. NTFS będzie dobrym wyborem jeśli wiesz, że dysk nie będzie używany na MacOS.

Następnie możesz nadać nazwę dyskowi – będzie się wyświetlać przy podłączeniu go do komputera. Wpisz nazwę w polu **Volume Label (Etykieta wolumenu)**.



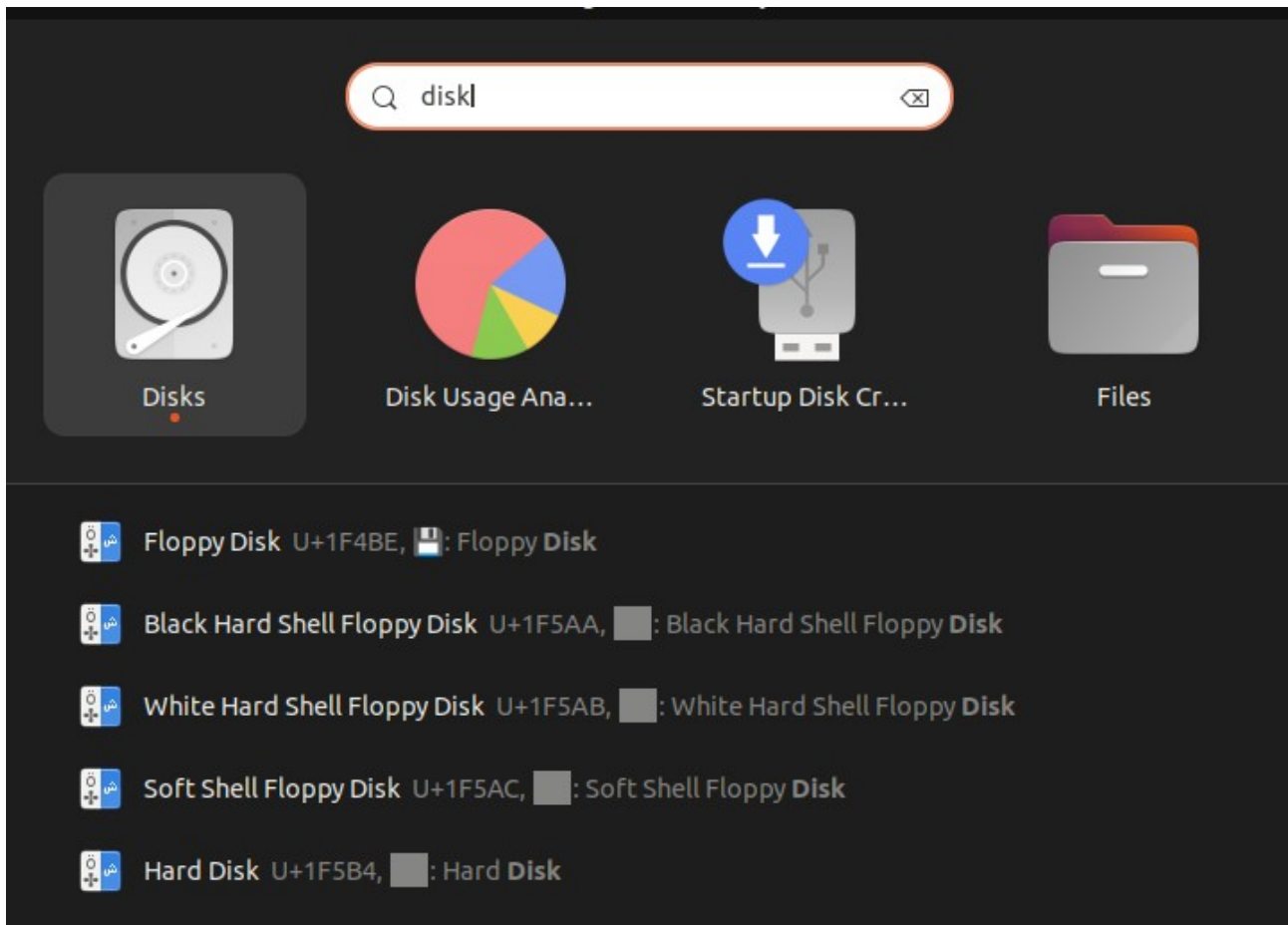
Kliknij `Next (Dalej)` i `Finish(Zakończ)` i gotowe, dysk wyczyszczony!

Linux (Ubuntu)

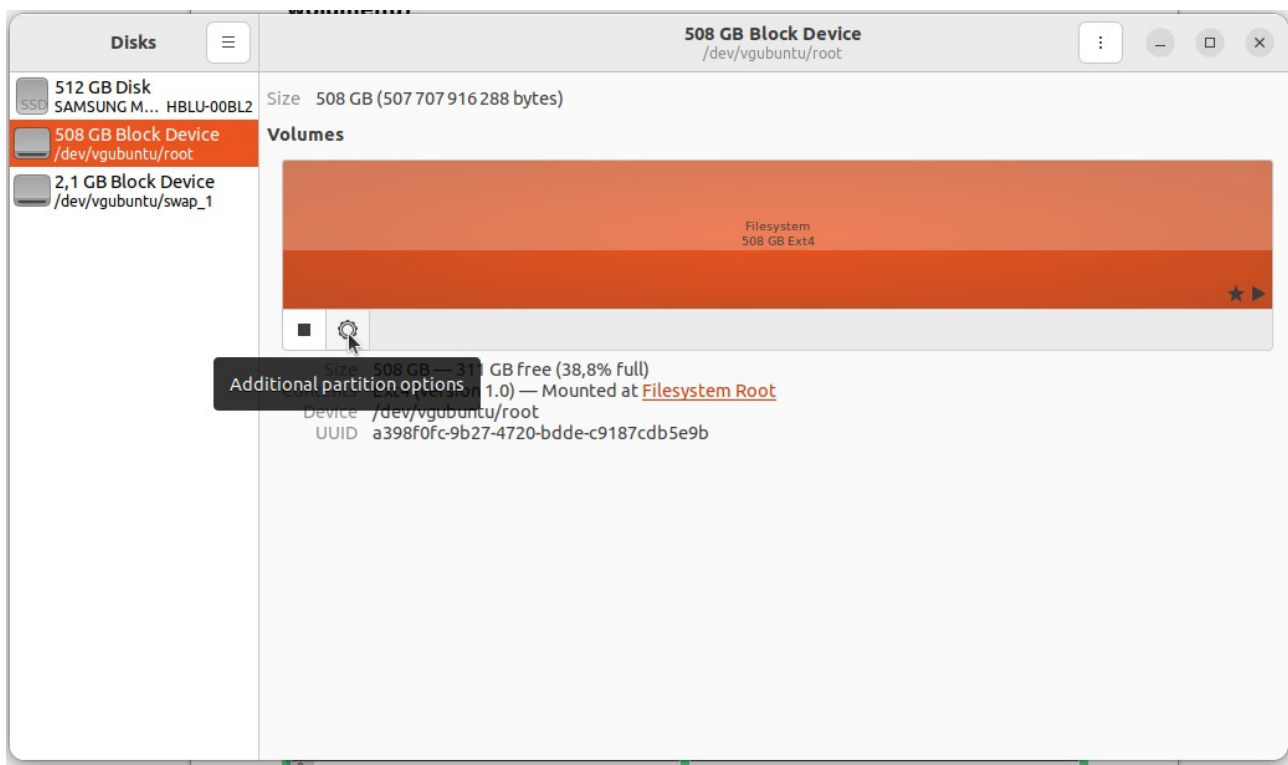
Otwórz

program

Disks.



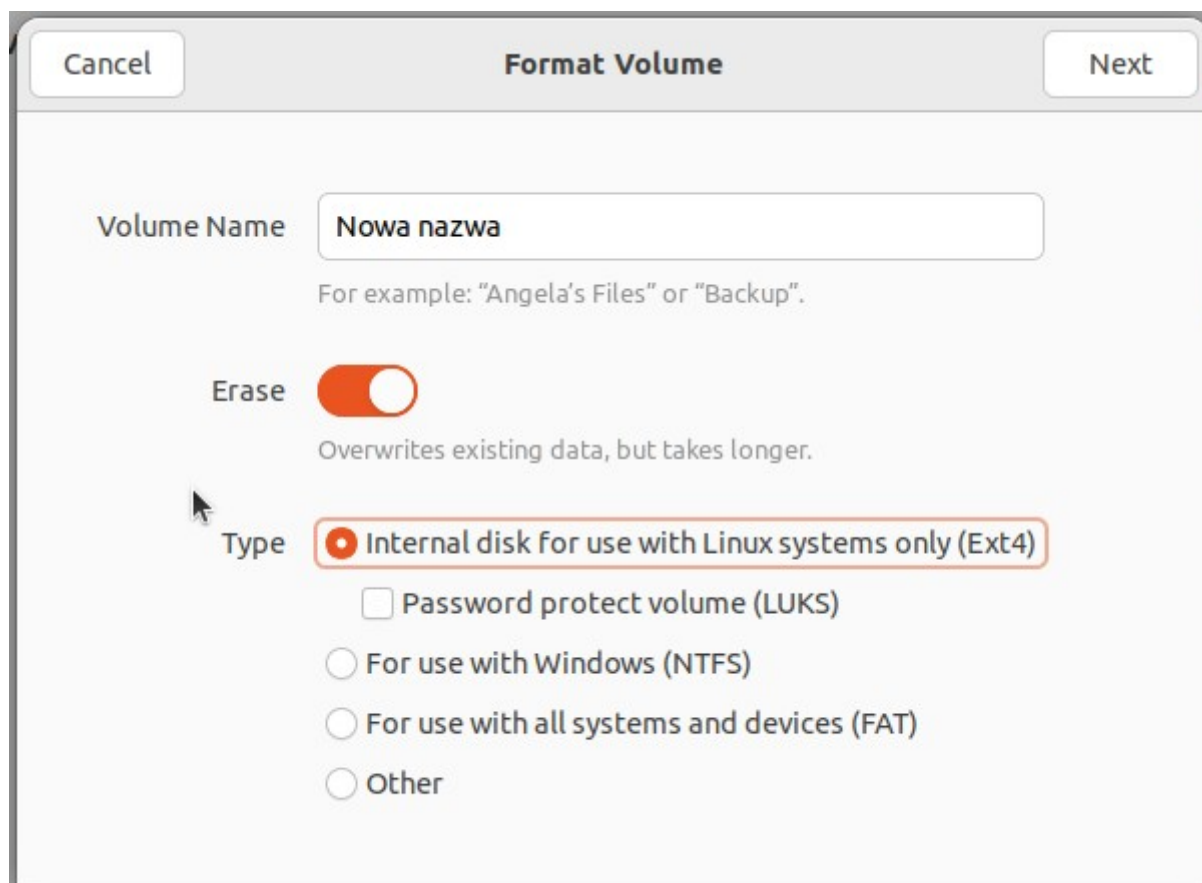
Zobaczysz listę dysków podłączonych w tym momencie do komputera. Żeby mieć pewność, że



czyścisz odpowiedni dysk, możesz odłączyć dysk zewnętrzny od komputera i sprawdzić, który dysk zniknął z listy – ten dysk nas interesuje.

Wybierz ikonę ustawień i opcję **‘Format partition (sformatuj partycję)’**.

Na kolejnym widoku możesz nadać nazwę dyskowi – będzie się wyświetlać po podłączeniu dysku do komputera. Wybierz też odpowiedni format systemu plików.



Wybierz Ext4, jeśli dysk będzie używany tylko z systemem Linux, NTFS, jeśli nie będzie wykorzystywany na MacOS, lub FAT, jeśli chcesz, żeby działał podłączony do dowolnego systemu operacyjnego. Następnie potwierdź swój wybór i kliknij **‘Format (Formatuj)’**. Proces trwa tym dłużej, im większy jest Twój dysk.

MacOS

Otwórz **/Aplikacje/Narzędzia/Narzędzie dyskowe**. Wybierz opcję **Widok ► Pokaż wszystkie urządzenia**. Zobaczysz listę dysków podłączonych do komputera. Wybierz dysk, który chcesz sformatować. Żeby mieć pewność, że czyścisz odpowiedni dysk, możesz odłączyć dysk zewnętrzny od komputera i sprawdzić, który dysk zniknął z listy – ten dysk nas interesuje.

Kliknij przycisk wymazania, wybierz z menu opcję 'Format' i wybierz format systemu plików. Jeśli dysk będzie używany tylko na komputerach z macOS nowszym niż 10.12, wybierz APFS. Jeśli dysk ma działać na wszystkich komputerach, niezależnie od systemu operacyjnego, wybierz NTFS.

Nadaj nazwę dysкови – będzie się wyświetlać po podłączeniu dysku do komputera. Kliknij 'Wymaż', a następnie 'Gotowe'. Dysk jest już czysty!

5.6 Jak bezpiecznie czyścić komputery

Przed sprzedażą komputera lub oddaniem go pracodawcy po zakończonej współpracy dobrze jest wyczyścić komputer – minimalizuje to ryzyko kradzieży twoich danych czy odtworzenia twojej historii przeglądania. Poniżej dostępne są linki do instrukcji w zależności od twojego systemu operacyjnego:

Linux

Linux jest darmowy, wobec tego jeśli masz w komputerze dodatkowe dyski poza tym, na którym zainstalowany jest system, wyczyść je zgodnie z instrukcją w punkcie 7.5, a następnie zainstaluj Linuxa od nowa. Oto instrukcja dla Ubuntu: <https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview>

Windows

<https://www.consumerreports.org/electronics-computers/computers/how-to-wipe-a-computer-clean-of-personal-data-a5849951358/>

MacOS

<https://www.backblaze.com/blog/how-to-wipe-a-mac-hard-drive/>

Następne rozdziały wkrótce!

Jeśli macie jakieś pytania, piszcie na:

kolektyw.rucajs@protonmail.com