

NASZE CYFROWE BEZPIECZEŃSTWO

Adam Jurkiewicz
Sekcja Informatyki Szkolnej przy PTI
adam.jurkiewicz.pythonista@pti.org.pl

Abstract. *In today's digital landscape, protecting our online identities has become more crucial than ever. Passwords, tokens, and security codes are essential tools in safeguarding our personal data from cyber threats. Embracing open source solutions empowers users to take control of their digital security with transparency and flexibility. This paper explores practical strategies for enhancing online safety using open source tools and best practices. By understanding and implementing these methods, we can build a safer digital environment for everyone.*

1. Wstęp

W dobie rosnących zagrożeń cyfrowych bezpieczne korzystanie z komputera to podstawa ochrony prywatności i danych osobowych.

To zapewne dość częste stwierdzenie, które czytamy lub słyszymy; i w sumie wydaje się być prawdziwe. Pozostaje zatem pytanie - w jaki sposób możemy owo "bezpieczne korzystanie" realizować w praktyce - jak się zabezpieczyć w duchu open source.? Większość z nas zapewne wie, że bezpieczny komputer to taki, który nie jest włączony do zasilania (nie działa), nie jest podłączony do sieci (nawet lokalnej, o Internecie nie wspominając), a najlepiej, gdy zakopieśmy go dodatkowo 20 metrów w głębokiej studni. No, tylko wtedy staje się dla nas trochę bezużyteczny.

Zatem postaramy się jednak działać tak - by można go było używać, a my byśmy czuli się bezpieczni. I to nie za miliony monet, tylko w miarę tanio. W tym artykule postaram się pokazać aplikacje, z których sam korzystam – legalne, darmowe:

- Linux Kubuntu - system operacyjny
- Brave Browser - przeglądarka internetu
- KeePassXC - aplikacja menadżera haseł
- Cryptomator - aplikacja tworząca zaszyfrowane sejfy (katalogi)

Wiem - zapewne w tej chwili większość pomyśli - Linuksiarz się znalazł... ale większość świata używa MacOS'a lub Windows'a ;-). Otóż uwaga - wszystkie opisywane przeze mnie aplikacje (poza systemem operacyjnym) są dostępne dla:

- Microsoft Windows

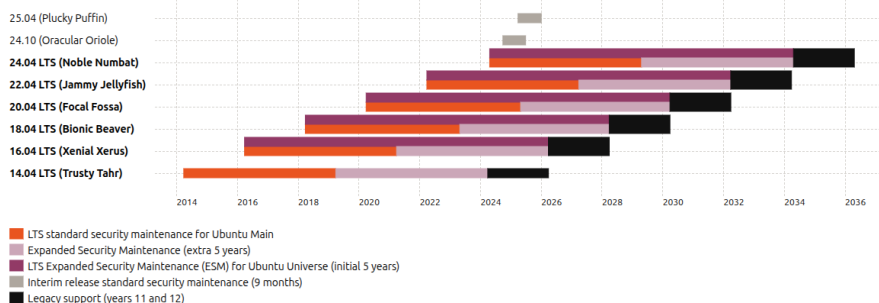
- macOS
- Linux

Tak, tak - najczęściej wybierając aplikacje OpenSource otrzymujemy produkt, który nas NIE ogranicza! Ale to oczywiście na pewno wiecie... Przyjdźmy zatem do omawiania tych elementów, które - przypomnę - sam używam, więc opisuję tu moje subiektywne odczucia! **#takpracuję**

2. Linux Kubuntu (system operacyjny) - <https://kubuntu.org/>

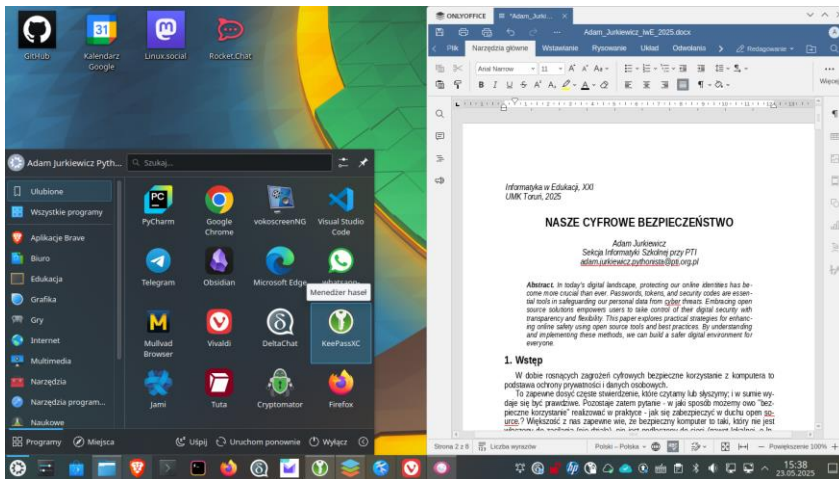
Kubuntu to przyjazna dystrybucja Linuxa z graficznym środowiskiem KDE, bazująca na Ubuntu, zapewniająca stabilność i bezpieczeństwo. Ja używam wersji 24.04 LTS – a więc dystrybucji ze wsparciem, jeśli chodzi o poprawki bezpieczeństwa, do 2029 roku w wersji darmowej, a w modelu płatnym do 2036 roku... Mnie osobiście rok 2029 wystarczy, gdyż wcześniej zmienię mojego Linuksa na kolejną wersję LTS, która powstanie - jak możecie zobaczyć, od wersji 14.04 (a ja używam Ubuntu od wersji 8.0) zawsze kolejna wersja LTS powstaje zanim poprzednia osiągnie koniec wsparcia bezpieczeństwa.

Ubuntu releases



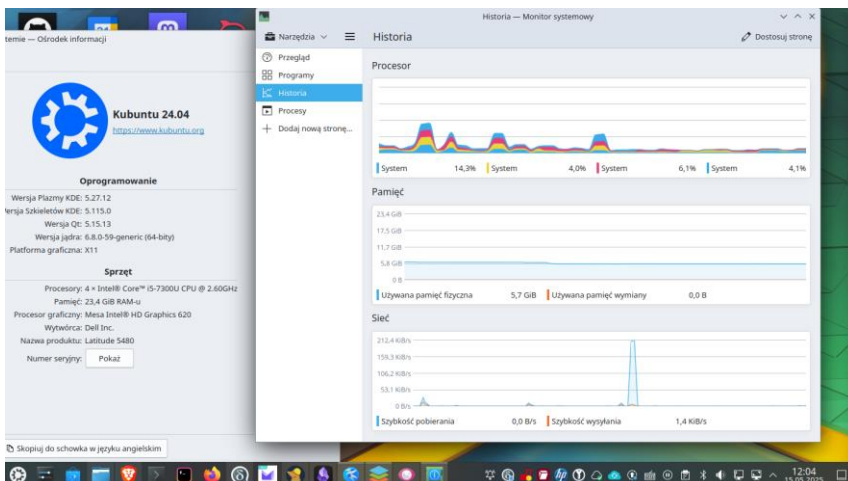
Rysunek 1. Czas wsparcia systemu Ubuntu

Poniżej możemy zobaczyć pulpit, na którym w połowie widać ten dokument w trakcie tworzenia (<https://www.onlyoffice.com/> - kolejna aplikacja OpenSource dla każdego) oraz menu aplikacji, gdzie widzimy przy okazji te aplikacje, z których korzystam najczęściej w mojej codziennej pracy.



Rysunek 2. Pulpit systemu Kubuntu Linux

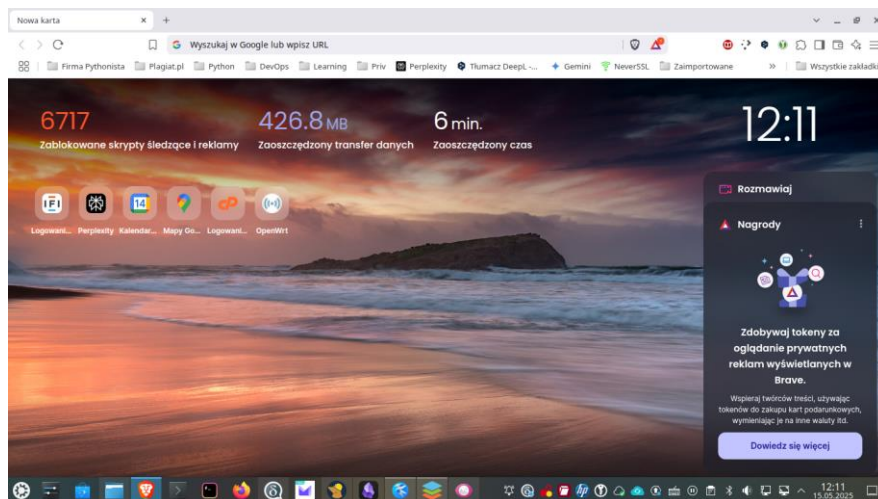
Nie będę przekonywał Was do używania tego systemu "zamiast" innego - jedynie pokażę, że wiele aplikacji jest w nim dostępnych. Nie działają tu wirusy pisane dla Windows, więc naprawdę trudno zainfekować go jakimś "ransomware"... Tak naprawdę, nie mam nawet antywirusa i jakoś mi to nie sprawia problemów. Komputer, który używam, nie jest najnowszy, a mimo to działa całkiem sprawnie.



Rysunek 3. Obciążenie systemu

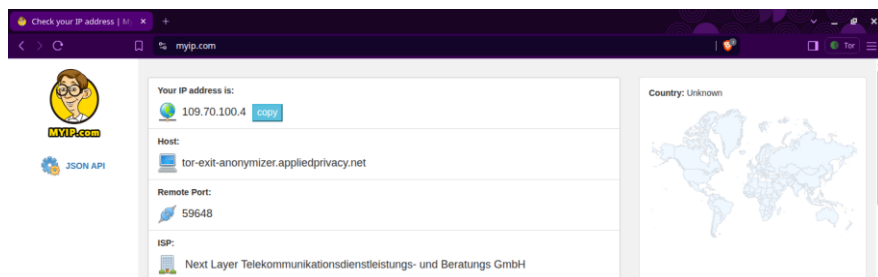
3. Brave Browser (przeglądarka WWW) - <https://brave.com/>

Przeglądarka oparta na Chromium, skupiająca się na ochronie prywatności i bezpieczeństwie użytkownika. Domyślnie blokuje reklamy, trackery i cyfrowe odciski palców.



Rysunek 4. Obraz przeglądarki w moim systemie

Używam jej do codziennego przeglądania internetu (ale nie do Facebooka, LinkedIn, Fediverse, BlueSky), również profil PTI oglądam w innej, jest szybka i wydajna, ma mniejsze wymagania niż Google Chrome czy Microsoft Edge.

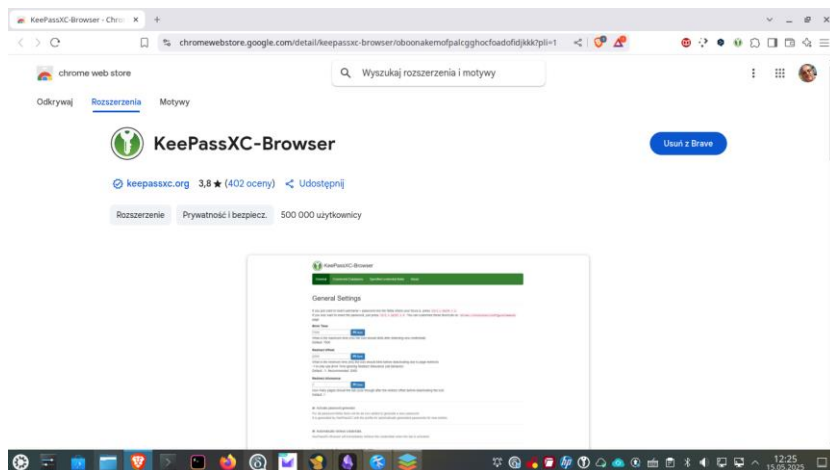


Rysunek 5. W trybie TOR nasz realny IP jest ukrywany

Oferuje tryb prywatny z Tor dla zwiększenia anonimowości. Możemy dzięki temu łatwo i szybko ukryć nasz prawdziwy IP. Nie wymaga do tego instalowania żadnych

dodatków; po prostu z menu wybieramy nową kartę prywatną z obsługą TOR. Wówczas, co widać na powyższym zrzucie, nagle zmieniamy lokalizację geograficzną, mamy więc możliwość "ukryć się" (**Country: unknown**) przed pewnymi narzędziami.

Oczywiście mam też zainstalowany dodatek, dzięki któremu mogę do niej pobierać hasła z **KeePassXC** (o którym za chwilę).

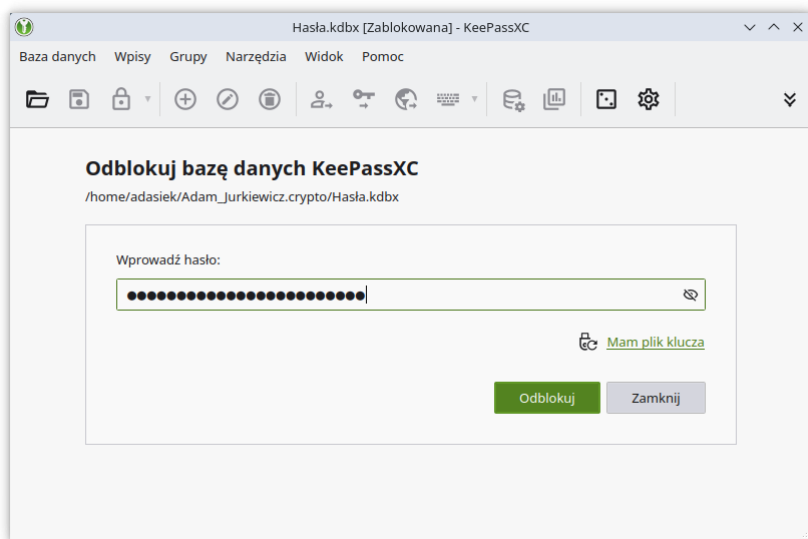


Rysunek 6. Rozszerzenie KeePassXC dla Brave

4. KeePassXC - (menadżer haseł) - <https://keepassxc.org/>

Menedżer haseł działający lokalnie, z silnym szyfrowaniem bazy danych (AES-256). Pozwala na generowanie silnych, unikalnych haseł, przechowywanie kodów TOTP do 2FA (dwuskładnikowe logowanie), integrację z przeglądarką (np. Brave). Ma możliwość zabezpieczenia bazy hasłem głównym oraz dodatkowo kluczem sprzętowym (np. Yubi-Key).

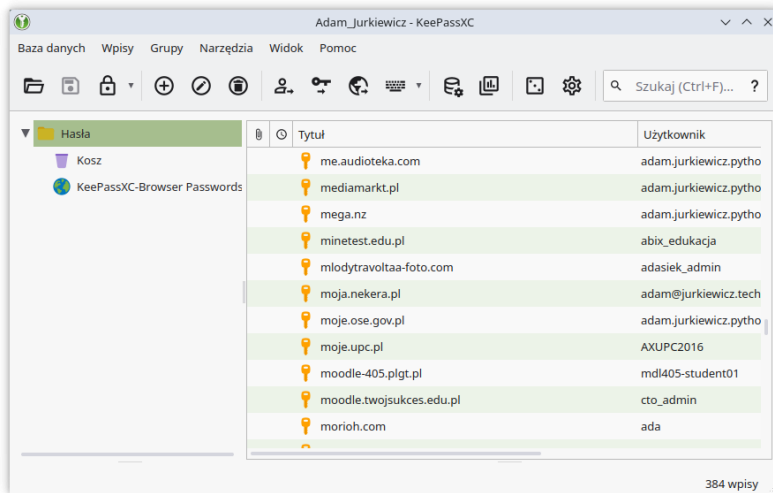
To suche zdania wygenerowane za pomocą modelu językowego (czyli potocznie sztucznej inteligencji).



Rysunek 7. Okno startowe KeePassXC

A moje subiektywne odczucia? Po prostu super aplikacja! Przede wszystkim, mamy Hasło główne, które jest wykorzystywane do szyfrowania pliku, który jest bazą danych - możemy spokojnie wysłać go do Chmury (np. ja używam pCloud ze Szwajcarii). Dzięki temu nawet, jeśli ktoś przechwyci ten plik, nie będzie mu łatwo go odczytać.

Aplikacja posiada generator haseł, dzięki któremu możemy tworzyć je unikatowo i bezpiecznie. Dla każdego serwisu mam inne hasło - i nawet, jeśli któryś ze sklepów, czy nawet sam Facebook - zaliczy wpadkę i wypłyną loginy i hasła - to najwyżej stracę jedno, a nie będę się zastanawiał, do ilu jeszcze serwisów uzyskają dostęp przestępcy.



Rysunek 8. Loginy i hasła - widok odblokowanej bazy

Na stronie Security (<https://www.security.org/how-secure-is-my-password/>) można spróbować "złamać" swoje hasło - w naszym przypadku to **2 decyliony lat** (nawet nie staram się przeliczyć, ile to czasu).



Rysunek 9. Strona obliczająca prawdopodobny czas złamania hasła

5. Cryptomator (szyfrowane katalogi) <https://cryptomator.org/>

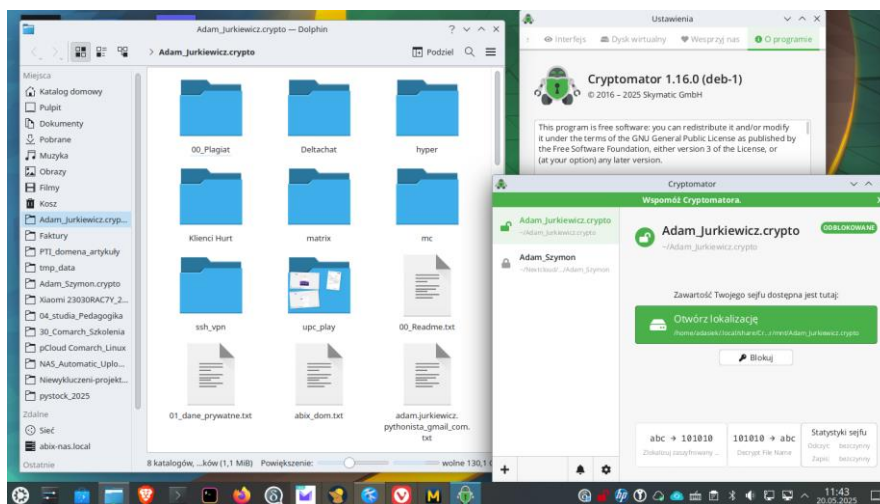
Nextcloud, GoogleDrive, iCloud, Dropbox, pCloud, oneDrive, SharePoint - chyba każdy z nas zna choć jedną z tych usług. Pięknie potrafią przechowywać nasze dane. Ale gdy chcemy je zaszyfrować, to albo jest to drogie, albo wręcz niemożliwe po stronie

dostawcy. Zwłaszcza, kiedy korzystamy z darmowych przestrzeni (np. 15 GB w Google, czy 10 GB w pCloud). W tym momencie przychodzi nam z pomocą Cryptomator.



Rysunek 10. Widok strony internetowej projektu

Na swojej stronie internetowej opisuje się dosyć dobrze, pozwala pobrać darmową aplikację, dzięki której tworzymy sejf - zaszyfrowany katalog.



Rysunek 11. Działająca aplikacja

Dla nas jest to po prostu katalog, w którym tworzymy kolejne, kopiujemy pliki. Na końcu jest automatycznie szyfrowany, i taki zaszyfrowany katalog możemy spokojnie

skopiować do chmury - używa algorytmu AES (Advanced Encryption Standard) z kluczem o długości 256 bitów (AES-256), który uznawany jest za jeden z najbezpieczniejszych obecnie dostępnych standardów szyfrowania

Na stronie <https://superbelfrzy.edu.pl/narzedzia/linux-i-wioo/cryptomator-jak-zabezpieczyc-swoje-dane-cz-1/> opisuję dokładniej, jak sobie tworzyć taki sejf.

6. Podsumowanie

Otwarte oprogramowanie (open source) daje transparentność i możliwość samodzielnej kontroli nad bezpieczeństwem. Połączenie **Kubuntu**, **KeePassXC**, **Brave** i **Cryptomator** tworzy wielowarstwową ochronę komputera i danych użytkownika. To chyba dobre podsumowanie; dodam, że czuję się bezpieczny wykorzystując te narzędzia w codziennej pracy.



Rysunek 12. Logo licencji GNU GPL 3

Korzystanie z GNU GPL wymaga, by wszystkie wydane ulepszone wersje były wolnym oprogramowaniem. To znaczy, że unikamy ryzyka konieczności konkurowania z prawnie zastrzeżoną zmienioną wersją swojej własnej pracy.

Nauczyciel może też z tego korzystać prywatnie, ale też służbowo - to Opensouce, a więc: legalne i darmowe oprogramowanie. Możemy również pokazywać je uczniom, wiele z ich funkcji pokrywa się wprost z zapisami podstawy programowej, jak np:

- Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym: znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

- Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Kończąc, zapraszam do kontaktu - oczywiście dzięki specjalnemu, szyfrowanemu komunikatorowi - DeltaChat.



Rysunek 13. QR Code do strony opisującej #DeltaChat

Literatura

1. Strony internetowe opisywanych projektów, ostatni dostęp maj 2025 roku.