
Menedżer haseł - Poradnik

Menedżer haseł – uruchamianie, używanie – kompletny **Poradnik**

W cyfrowym świecie dane są zabezpieczone hasłami.

Dostęp do poczty, do serwisu społecznościowego itd. Wymaga podania loginu i hasła.

Takich miejsc, do których potrzebujesz loginu i hasła każdy ma dziesiątki.

Zgodnie z praktykami w bezpieczeństwie posiadanie jednego, dwóch, a nawet pięciu haseł i ich mutacji nie jest najlepszym wyborem.

Z drugiej strony jesteśmy ludźmi, którzy inaczej niż komputery zapamiętują informacje i jest dla nas trudnością spamiętać 20, 50, 100 różnych haseł.

Przychodzą z pomocą odpowiednie narzędzia, nazywane także programami, usługami, serwisami, które wykonują tą pracę za ludzi.

Wsparciem dla samych haseł są dodatkowe zabezpieczenia, które opierają się na dodatkowym składniku logowania.

Moment kiedy jest potrzeba użycia hasła, miejsce w którym tego dokonujemy i urządzenia z którego się to wykonuje komplikuje nieco sytuację i stwarza różne zagrożenia.

Menedżer haseł pozwala zalogować się tam gdzie jest potrzeba, spełniając odpowiednie kryteria bezpieczeństwa.

W tym poradniku dostaniesz instrukcje, opis powodu kiedy, jak i dlaczego używać opisanego sposobu, konfiguracji, ustawienia lub narzędzia, by jeszcze jaśniej pokazać dlaczego powinno się tak robić.

Poradnik od początku do końca zawiera bardzo dokładne instrukcje, by nie pozostawić niedomówień, a odbiorca był prowadzony za rękę przez cały proces.

Sukcesem poradnika będzie sytuacja kiedy po wykonaniu jakiejś czynności stwierdzisz, że był to proste, łatwe i skuteczne, a gdy trzeba będzie zrobić coś jeszcze raz, od początku nawet bez poradnika zrobisz to intuicyjnie.

Jako autor wierzę, że dasz radę zrobić wszystko od początku do końca a używanie menedżera haseł będzie przyjemne i proste.

Mając z tyłu głowy potrzebę odsunięcia zagrożeń związanych z hasłami, zaczniesz używać menedżera haseł z lenistwa bo będzie to dla Ciebie prostsze niż usiłowanie stworzenia, zapamiętania i wprowadzenia hasła w dowolnym miejscu gdzie będzie ono strzegło poufności danych, tożsamości i informacji w twoim życiu osobistym i zawodowym.

Powodzenia!

Artur Markiewicz

W wielu miejscach poradnika znajdziesz aktywne odnośniki do innych części wyglądające jak ten  [np. ten, który przeniesie Cię na górę](#) tej strony, lub w dolnej części znajdziesz odnośnik do [MENU](#), który jak teraz klikniesz, to przeniesie Cię na kolejną stronę poradnika😊

Spis treści

Menedżer haseł – uruchamianie, używanie	1
1. Profil odbiorcy	4
2. Cel stworzenia dokumentu i jego zawartość	4
2.10. Wersja dokumentu.....	4
2.11. Plany rozbudowy dokumentu	4
3. Dlaczego menedżer haseł?.....	5
3.1. Po co są hasła?	5
3.2. Wycieki haseł	5
3.3. Sprawdzanie czy moje hasła wyciekły	5
3.4. Zalety menedżera haseł	6
3.5. Inne możliwości.....	6
4. LastPass – dlaczego ten wybór?.....	7
4.1. Argumenty przemawiające za wyborem LastPass:.....	7
4.2. Kiedy LastPass nie jest najlepszym wyborem?	7
4.3. Bolączki wszystkich narzędzi typu menedżer haseł	8
5. Rejestracja i instalacja LastPass na komputerze	9
6. Instalacja LastPass na telefonie Apple – iPhone	20
7. Używanie LastPass na komputerze	32
7.1. Domyślny widok LastPass w przeglądarce	32
7.2. Edycja wpisów w LastPass.....	33
7.3. Dodawanie ręcznie haseł	35
8. Używanie LastPass na stronie internetowej	38
8.1. Generowanie bezpiecznych haseł.....	40
9. Instalacja LastPass na telefonie Android.....	43
10. Podnoszenie bezpieczeństwa menedżera haseł.....	51
10.1. Wchodzenie do ustawień konta.....	52
10.2. Włączanie drugiego składnika logowania w postaci Microsoft Authenticator	55
10.3. Włączanie drugiego składnika logowania w LastPass Authenticator.....	61
10.4. Alternatywna forma drugiego składnika logowania	66
10.5. Aby komputer (lub telefon) pamiętał drugi składnik logowania przez 30 dni	67
10.6. Czas kiedy LastPass się wyloguje.....	68
11. Jednorazowe hasła logowania do LastPass.....	70
11.1. Generowanie jednorazowych haseł OTP	70
11.2. Jak wykorzystać OTP w praktyce.....	72
12. Podsumowanie.....	75

1. Profil odbiorcy

- 1.1. Użytkownik urządzeń (komputer, tablet, smartphone itd.), który nie korzystał do tej pory z menedżera haseł i chce lepiej zabezpieczyć swoje dane do logowania do urządzeń i do serwisów/platform,
- 1.2. Osoba, która chce nauczyć się używania menedżera haseł,
- 1.3. Odbiorca używający do zarządzania hasłami wielu urządzeń (komputer, tablet) w różnych środowiskach systemów operacyjnych (Windows, OSX – iPhone, Android),

2. Cel stworzenia dokumentu i jego zawartość

Motywacją do stworzenia poradnika było przedstawić zagadnienia związane z zarządzaniem hasłami w cyfrowym świecie jest koniecznością i można zrobić to w bardzo łatwy sposób.

- 2.1. Przybliżenie odbiorcy poradnika tematyki zarządzania hasłami, obsługi wielu różnych i skomplikowanych haseł,
- 2.2. Wprowadzenie do tematyki zarządzania hasłami, obsługi wielu różnych i skomplikowanych haseł
- 2.3. Pomoc w poszerzeniu wiedzy o bezpieczeństwie i zminimalizowaniu zagrożeń,
- 2.4. Propagowanie wiedzy o bezpieczeństwie i minimalizowania zagrożeń związanych z wyciekami haseł,
- 2.5. Zapoznanie z jedną z dostępnych na rynku aplikacją do zarządzania hasłami,
- 2.6. Nauczenie odbiorcę dokumentu obsługi jednego z programów do zarządzania hasłami – menedżera haseł **LastPass**,
- 2.7. Pokazanie idei i praktycznego zastosowania wieloskładnikowego logowania,
- 2.8. Nauczenie jak, kiedy i dlaczego korzystać z jednorazowych haseł dostępu do menedżera haseł,
- 2.9. Opisujący tutaj **LastPass** jest pozbawiony polskiej wersji językowej, stąd szczegółowość opisów, instrukcji oraz mnogość zrzutów ekranu, które pokazują ustawienie domyślne i docelowe po wprowadzeniu omówionego kroku obsługi.

2.10. Wersja dokumentu

- 2.10.1. Wersja 0,7 – pierwsza wersja z opisem wersjonowania

2.11. Plany rozbudowy dokumentu

- 2.11.1. Wersja 0,8 – wersja po opinii testerów z naniesionymi zmianami
- 2.11.2. Wersja 1,0 – dla komercyjnych odbiorców zawierająca poprawki, jednolity styl i formatowanie dokumentu
- 2.11.3. Wersja 1,5 – opisane funkcjonalności
 - 2.11.3.1. udostępnianie haseł
 - 2.11.3.2. aplikacja zainstalowana lokalnie na komputerze
 - 2.11.3.3. używanie wypełnienia pól związanych z kartami płatniczymi
 - 2.11.3.4. automatyczna zmiana haseł w portalach
 - 2.11.3.5. bezpieczne notatki
 - 2.11.3.6. zaawansowane funkcje zarządzania dostępem do menedżera haseł
 - 2.11.3.7. import baz z hasłami z innych źródeł
- 2.11.4. Wersja 2,0 – opisane funkcjonalności PREMIUM
- 2.11.5. Wersja 2,0 – opisane funkcjonalności Families
W zakresie szaty graficznej całego dokumentu
- 2.11.6. Wersja x,x z literką małą – dla testerów - wersja w szacie graficznej na miarę XXI. wieku
- 2.11.7. Wersja x,x z literką DUŻĄ – dla odbiorców wersja w szacie graficznej na miarę XXI. wieku

3. Dlaczego menedżer haseł?

3.1. Po co są hasła?

Do ochrony kont internetowych, tożsamości potrzeba dwóch danych: loginu (najczęściej to adres mail) oraz hasła.

Każdy z nas ma od kilkunastu do kilkudziesięciu miejsc gdzie takie dane są potrzebne.

O ile adres mail pamiętamy i może być jeden do wszystkiego, o tyle hasło nie powinno być wszędzie takie samo.

Pan z wąsem podczas szkolenia z RODO, czytając kolejny slajd, zwiększając poziom nudy zapewne powiedział: „hasło ma mieć 9 znaków, w tym cyfry, litery, znaki specjalne małe i duże litery”. Jedno, dwa, pięć można spamiętać, ale 41? Stąd zastana sytuacja, że używamy jednego, dwóch haseł z małymi modyfikacjami. Dla systemów komputerowych to wystarczy, dla całościowego bezpieczeństwa nie.

3.2. Wycieki haseł

Nie masz wpływu na to czy twoje hasło Alicja2011 wyciekło z jakiegoś sklepu internetowego gdzie go używasz.

Masz wpływ na to, że taki wyciek nie będzie mieć wpływu na inne konta w sieci.

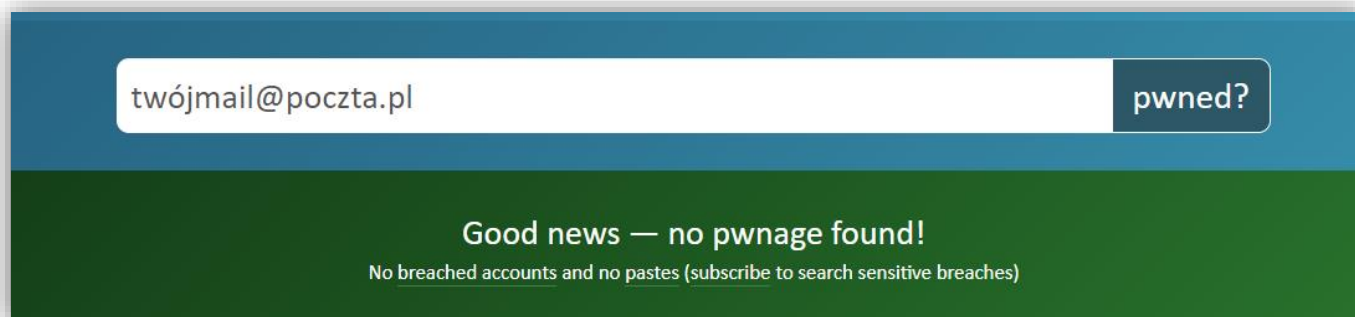
Jeśli przestępcy znają hasło z wycieku, to mogą je zastosować do innych ataków. Np. jak ten na pewien sklep z meblami <https://cyberkurs.online/powinni-to-drukowac-na-opakowaniach-od-hotdoga>

3.3. Sprawdzanie czy moje hasła wyciekły

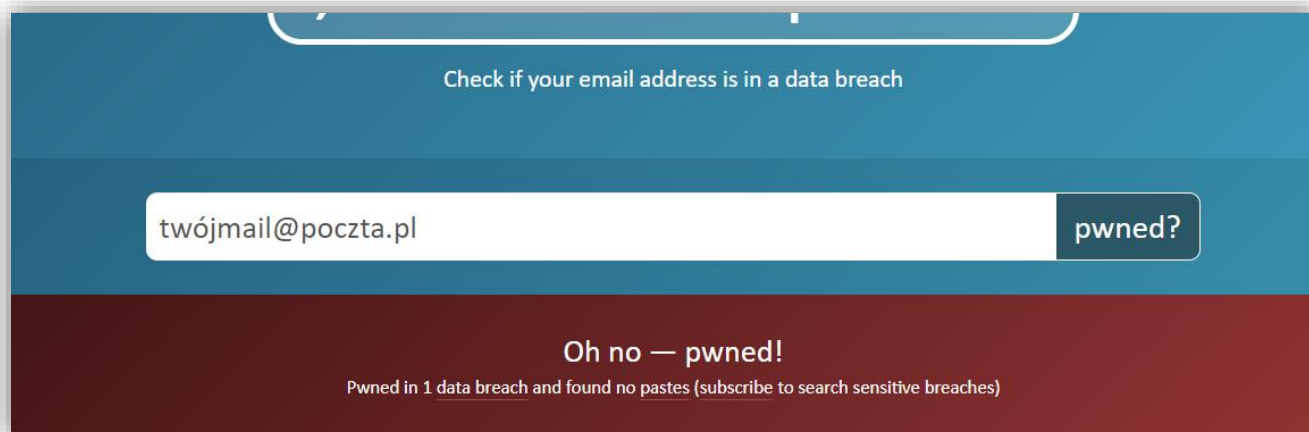
Możesz sprawdzić czy Twoje dane logowania związane mailem, który jest identyfikatorem wyciekły.

Wpisz swój adres mailowy w wyszukiwarce na tej stronie <https://haveibeenpwned.com/>

Jeśli po wpisaniu maila i wyszukaniu ekran jest zielony, to jest ok.



Jeśli ekran zrobił się czerwony to znak, że gdzieś w sieci krążą twoje hasła.



Możesz doczytać z jakiego miejsca, kiedy, co i w jakich okolicznościach wyciekło.

Badacze prowadzą takie zestawienia, a wymieniona wyszukiwarka pozwala zapoznać się z tymi informacjami w kontekście własnych loginów i danych.

3.4. Zalety menedżera haseł

Dzięki menedżerowi haseł będziesz mieć wszędzie różne hasła, co redukuje do zera możliwość ich stosowania przez hakerów nawet gdy wyciekną.

Menedżer haseł pozwoli Ci przechowywać wszystkie wprowadzone hasła w bezpiecznej pamięci tego oprogramowania (usługi, systemu w zależności od narzędzia).

Menedżer haseł nie zasugeruje, nie uzupełni automatycznie hasła w sytuacji gdy nie jesteś na prawdziwej stronie, na której chcesz być, lub wydaje się Tobie, że jesteś.

Jeśli masz wątpliwości czy menedżer haseł jest bezpieczny, to zastanów się co stwarza większe ryzyko: posiadanie kilku haseł, które mogą być przewidywalne czy włamanie do firmy, która głównie się zajmuje bezpieczeństwem.

Owszem, jest to możliwe, że nastąpi ujawnienie podatności (dziur w oprogramowaniu, sposobu dostania się do bazy) mające konsekwencje w postaci ujawnienia haseł, jednak jest ono bardzo niskie, o wiele niższe niż ujawnienie hasła, które przypadkiem pasuje do wielu innych miejsc.

Proponuję w tym poradniku konkretny menedżer haseł **LastPass**.

Przeczytasz o nim w kolejnych punktach, a idąc krok po kroku w tej instrukcji nauczysz się go używać.

3.5. Inne możliwości

Stosowanie narzędzia, które pamięta za Ciebie danych do logowania się, stwarza możliwość stosowania różnych loginów w trosce o jeszcze większe bezpieczeństwo.

Masz możliwość zakładania kont osobno na adres prywatny, osobno na adres służbowy w zależności od miejsca gdzie ma być założone.

Np. jako autor bloga możesz używać konta pocztowego dedykowanego do tego obszaru życia w sieci, używając tożsamości auto@nazwabLOGA.pl a konto na portalu dla hobbystów założyć konto na inny adres mail np. rybak2000@wp.pl

Dla rodziny nadal pozostaniesz jako adam1990@wp.pl a dla pracodawcy adam.kowalski@gmail.com

Jak widzisz jest całe spektrum możliwości by nie musieć pamiętać a móc używać.

4. LastPass – dlaczego ten wybór?

Jest wiele menedżerów haseł a ten został wybrany z kilku powodów.

4.1. Argumenty przemawiające za wyborem LastPass:

4.1.1. Jest intuicyjny w obsłudze,

4.1.2. Jest chmurowy* co pozwala na używanie go na wszystkich urządzeniach po zalogowaniu się w dedykowanej aplikacji. Synchronizacja danych trwa sekundy, więc po wprowadzeniu do menedżera danych logowania do serwisu internetowego, na drugim urządzeniu po kilku sekundach też się zalogujesz,

**chmurowy czyli oparty o serwisy producenta, które udostępniają twoje dane menedżera haseł, między twoim oprogramowaniem na twoim sprzęcie;*

4.1.3. W opcji bezpłatnej* nie ma ograniczeń co do przechowywanych haseł, ilości urządzeń na których się pracuje,

**O takiej jest narracja całego dokumentu, a zrzuty ekranu zawierające wersję rpońna PREMIUM są naturalne, gdyż każdy po rejestracji taką dostaje na start, gdy ona się skończy pozostaje opisana funkcjonalność;*

4.1.4. Można wykonać lokalną kopię zapasową zgromadzonych danych.

Taka kopia pozwala odzyskać wszystkie dane, mieć do nich wgląd i możliwość edycji oprogramowaniem typu arkusz kalkulacyjny na komputerze;

Taka kopia jako plik wymaga szczególnej ochrony, którą możesz zrealizować np. poprzez przechowywanie jej na pendrive (najlepiej szyfrowanym) w sekretnym miejscu;

4.1.5. Podstawowa funkcjonalność to wypełnienie pól logowania do strony internetowej (uzupełnienie loginu i hasła) bazuje na weryfikacji prawdziwości strony internetowej.

LastPass nie uzupełni automatycznie hasła do strony, która pozornie jest stroną Facebooka, gdyż on widzi „po swojemu” jakie to dokładnie miejsce w Internecie.

Np. jeśli jesteś na stronie [www.Fac3b00k.com](#), którą stworzyli przestępcy w celu wyłudzenia hasła, to twój wzrok może odnieść wrażenie poprawności, jednak **LastPass** nie uzupełni loginu dla zapamiętanej strony [www.facebook.com](#)

4.1.6. Pozwala wprowadzać w przeglądarce dane logowania, karty płatnicze, dane osobowe, które zapamiętał. *Ułatwia to wypełnianie wielu formularzy przy realizacji zamówienia, płatności, pism w wersji elektronicznej w wypełnianych w przeglądarce.*

4.1.7. Bardzo klarownie opisują swoją politykę bezpieczeństwa, którą [możesz przeczytać tu](#)

4.2. Kiedy LastPass nie jest najlepszym wyborem?

4.2.1. Gdy pracujesz tylko na jednym urządzeniu i pracowanie na lokalnej bazie z hasłami nie przeszkadza Ci w pracy. Zdecydowanie lepsze będą inne menedżery haseł do takiego typu pracy, które bazują na idei zainstalowanego oprogramowania i bazie z hasłami, które z założenia nigdy nie potrzebują dostępu do Internetu do zrealizowania swojej pracy.

4.2.2. Gdy przechowujesz w nim szczególnie chronione dane, których pozyskaniem są zainteresowani adwersarze publiczni i/lub ponadnarodowi – rządy i służby.

Tutaj ryzyko udzielenia dostępu wykorzystując prawne możliwości takiego aktora, który urzędowo może wywierać presję na producenta, a ten mimo zarzekania się, że nie ma takiej możliwości, może ulec takiemu naciskowi.

W takiej sytuacji menedżer haseł jest jednym z wielu narzędzi, praktyk i sposobów by zmniejszać ryzyko wycieku danych w takich okolicznościach i lepiej stosować inne, zainstalowane lokalnie.

Opisani powyżej adwersarze zajmują się sprawami dotyczącymi szpiegostwa, terroryzmu, handlu ludźmi/narkotykami.

4.3. Bolączki wszystkich narzędzi typu menedżer haseł

4.3.1. Każdy system jest tak długo bezpieczny, aż ktoś nie będzie miał dostępu do twoich danych.

Dotyczy to także menedżera haseł (każdego).

4.3.2. Jeśli będzie dostępne dla innych główne hasło, zarchiwizowana baza z hasłami, lub podatności w oprogramowaniu, na którą nie masz wpływu to tracisz kontrolę nad swoją prywatnością.

Znaczną część ryzyk możesz zniwelować poprzez drugi składnik logowania, którym będzie SMS, token sprzętowy lub programowy, biometria, klucz sprzętowy. Opisane to jest w części [Podnoszenie bezpieczeństwa menedżera haseł](#)  (kliknij by się tam przenieść)

LastPass łączy w sobie wiele zalet specyficznych dla oprogramowania (zwanych również jako: rozwiązania, systemy, technologie), ułatwiającym bezpieczną pracę z hasłami na wielu urządzeniach jednocześnie, w intuicyjny sposób.

Z dalszej części dokumentu dowiesz się:

-jak zarejestrować się w LastPass

-jak zainstalować to oprogramowanie na telefonie i komputerze

-jak podnieść bezpieczeństwo menedżera haseł

Aby go zdobyć w pełnej wersji, sprawdź tą stronę [Menedżer haseł - poradnik - szkolenia z cyberbezpieczeństwa \(cyberkurs.online\)](#)

