

Prezes UODO promuje testowanie haseł

Posted on 2026-10-01

Wprowadzenie w Polsce aplikacji FantomApp, która pomaga nastolatkom (a także dorosłym) lepiej dbać o swoje bezpieczeństwo w sieci, stanowi okazję do ponownego przyjrzenia się zagadnieniu ustawiania haseł, sposobom zarządzania nimi, ich właściwościom oraz zintegrowanemu z aplikacją narzędziu „Testuj hasło”.

Aplikacja FantomApp zawiera narzędzie do sprawdzania haseł. Ta funkcja może budzić wątpliwości u osób, które nie rozumieją, w jaki sposób obliczane są sugerowane wyniki. Przyjrzyjmy się bliżej hasłom, ich tworzeniu, przechowywaniu oraz sposobowi, w jaki narzędzie to przeprowadza obliczenia.

Z czego składa się FantomApp?

W sierpniu 2026 r. wprowadzono dla użytkowników w Polsce aplikację FantomApp, o czym informował już Prezes UODO na stronie internetowej Urzędu. Aplikacja została opracowana przez CNIL w ramach projektu finansowanego przez Unię Europejską. FantomApp ma na celu wsparcie osób z niej korzystających w zakresie zwiększenia bezpieczeństwa w sieci, głównie w ramach korzystania z mediów społecznościowych.

Aby to osiągnąć, FantomApp udostępnia kilka modułów:

- „Mam problem w Internecie”: sekcja poświęcona zasobom, z których można skorzystać w potencjalnie problematycznych sytuacjach w sieci, niezależnie od tego, czy chodzi o usunięcie treści, kradzież tożsamości, czy nawet szantaż seksualny. Różne zakładki pozwalają użytkownikom uzyskać dostęp do niezbędnej pomocy za pomocą jednego kliknięcia.
- „Narzędzia”: ta sekcja oferuje trzy narzędzia do sprawdzania i poprawiania bezpieczeństwa w sieci: narzędzie do sprawdzania haseł, narzędzie do rozmywania zdjęć oraz kwestionariusz dotyczący danych osobowych zawartych w nazwach użytkownika/opisach na profilach w mediach społecznościowych. Wszystkie narzędzia działają lokalnie, bez przysyłania danych na serwery. Użytkownicy mogą zatem sprawdzać swoje hasła i rozmywać zdjęcia z zachowaniem pełnej poufności.
- „Bądź bezpieczny”: ten moduł zawiera listę najpopularniejszych serwisów społecznościowych i prowadzi użytkowników przez ich ustawienia za pomocą zrzutów ekranu, aby poprawić ich prywatność w sieci. Listy kontrolne przygotowywane są w oparciu o dostępne opcje (lokalizacja, bezpieczeństwo, widoczność, dobre praktyki).

Czym jest silne hasło i jak je stworzyć?

Posiadanie silnego hasła jest niezbędne, ale co to właściwie oznacza? Często zaleca się przestrzeganie takich wytycznych, jak m.in.:

- 1 cyfra
- 1 wielka litera
- 1 znak specjalny

- Co najmniej 8, 10 lub 12 znaków.

Większość stron internetowych lub serwisów społecznościowych, na których zakładamy konta, wymusza przestrzeganie tych zasad, co czasami może dawać fałszywe poczucie bezpieczeństwa, nie uwzględniając przy tym optymalnej kombinacji tych czynników.

Aby określić siłę hasła, można posłużyć się pojęciem entropii, dostosowanym do tego konkretnego kontekstu. To obiektywna i łatwa do obliczenia miara, która odpowiada wszystkim możliwym kombinacjom, jakie może przyjąć hasło. Służy ona jako górna granica przy szacowaniu czasu potrzebnego do „złamania” hasła.

W kontekście tworzenia silnego hasła należy przestrzegać również innych zasad, takich jak unikanie używania własnego imienia, imion dzieci czy imion zwierząt domowych.

Na czym polega łamanie haseł?

„Prawdziwi” hakerzy korzystają bowiem z gotowych list haseł, które pozwalają im wypróbować ogromną liczbę różnych kombinacji. Listy te mogą nawet zawierać kombinacje wielu słów, połączenia ich z cyframi, lub zastąpienie np. litery „a” symbolem „@” i tak dalej.

Co więcej, cyberprzestępcy wykorzystują również listy haseł pochodzące z wycieków danych zawierające informacje z kont, na które już dawno ktoś przestał się logować, ale..., obecnie używa tego samego hasła np. w swojej ulubionej sieci społecznościowej. Dlatego zalecane jest, aby nie używać tego samego hasła na wielu stronach.

Należy zachować ostrożność w przypadku internetowych narzędzi do sprawdzania haseł: nie zaleca się testowania haseł na przypadkowych lub niesprawdzonych stronach. Jeśli nie ma

pewności, czy dane nie są przesyłane na serwery tej strony, nie ma jednocześnie gwarancji, że hasła nie zostaną wykradzione. Takie listy haseł mogą być następnie sprzedawane na platformach wymiany danych wśród hakerów.

FantomApp pozwala na bezpieczne sprawdzanie siły hasła

W aplikacji FantomApp – ponieważ kod źródłowy jest otwarty – można sprawdzić (lub poprosić o to eksperta), czy wszystkie dane pozostają lokalnie na telefonie użytkownika. Twórcy postanowili dodać pole wyboru podczas tworzenia hasła: „zawiera moje imię, nazwisko lub łatwe do odgadnięcia słowa”. Chociaż aplikacja nadal oblicza klasyczną entropię, to pole wyboru pozwala jej zaznaczyć wszystkie przypadki, w których haker mógłby odgadnąć hasło lub skorzystać z gotowej listy haseł. W takich przypadkach szacowany czas złamania hasła jest zawsze wyświetlany jako „natychmiastowy”.

Pojawiło się kilka uwag dotyczących promowania przez Prezesa UODO aplikacji FantomApp. Aby przeliczyć siłę hasła na szacowany czas, aplikacja korzysta z macierzy obliczonej przez Hive System – firmę zajmującą się cyberbezpieczeństwem, która co roku szacuje, ile czasu zajęłoby złamanie hasła na podstawie jego długości i składu (wielkie litery, cyfry, znaki specjalne itp.). Macierz wykorzystana w aplikacji FantomApp jest dostępna na stronie internetowej firmy.

Ograniczenia aplikacji FantomApp

Można to sprawdzić samodzielnie: 14-znakowe hasło zawierające wielkie i małe litery, cyfry oraz znaki specjalne wykazuje w macierzy wartość „19 tn lat”, co przekłada się na „19 bilionów lat”. Oczywiście szacunki te mają pewne ograniczenia, które firma Hive System przedstawia na swojej stronie internetowej:

- Zakładają one, że hasło użytkownika nie padło ofiarą wycieku danych, w wyniku którego mogłoby zostać odzyskane w postaci zwykłego tekstu
- Zakłada się, że hasło jest generowane losowo, co oznacza, że haker nie jest w stanie go odgadnąć, a atakujący musiałby wypróbować wszystkie możliwe kombinacje – jest to swego rodzaju „najgorszy scenariusz”, określający górną granicę czasu, jaki zajęłoby atakującemu złamanie hasła
- Wykorzystuje się klawiaturę QWERTY, bez znaków diakrytycznych powszechnie używanych zarówno w języku polskim, jak i w języku francuskim. To ograniczenie zmniejsza potencjalną siłę hasła
- Inne ograniczenia zostały wymienione na stronie internetowej firmy.

Kiedy haker próbuje odgadnąć hasło, zwykle nie próbuje zalogować się na konto w mediach społecznościowych, testując hasła jedno po drugim. Zazwyczaj użytkownik ma trzy próby, zanim zostanie zablokowany, a po ich wyczerpaniu otrzyma powiadomienie. Dlatego hakerzy próbują odzyskać hasła z baz danych, które wyciekły – jest to znacznie łatwiejsze.

Skróty haseł mają zwiększyć skuteczność zabezpieczeń

Gdyby hasła nie były zaszyfrowane za pomocą funkcji skrótu (inaczej funkcji haszującej), matryca systemu Hive straciłaby sens, ponieważ wszystko odbywałoby się „natychmiastowo” – haker musiałby jedynie odczytać zawartość bazy danych. Dlatego ważne jest, aby zrozumieć mechanizmy leżące u podstaw przechowywania haseł oraz powody, dla których złamanie ich może zająć hakerom sporo czasu.

W wielu przypadkach hasła są przechowywane w bazach danych w postaci skrótów (choć niektóre strony nadal nie stosują funkcji skrótu, jest to coraz radsze zjawisko). Baza danych, która wyciekła nie zawiera haseł w postaci zwykłego tekstu, czyli w formie czytelnej, lecz ich skróty, które wyglądają jak bezsensowny ciąg znaków. Kiedy użytkownik loguje się na stronie, hasło jest najpierw poddawane funkcji skrótu, a następnie porównywane ze skrótem przechowywanym w bazie danych. Oczywiście, gdyby użytkownik próbował wprowadzić sam skrót zamiast hasła, aby się zalogować, zostałoby to odrzucone.

Jednak ten środek bezpieczeństwa nie jest pozbawiony wad. W rzeczywistości każdy może skorzystać z funkcji haszującej. W rezultacie istnieją tabele odnośników, które kojarzą powszechnie używane hasła z odpowiadającymi im skrótami. Są one znane jako tabele Rainbow. Hakerzy wykorzystują je na listach znanych haseł, a następnie mogą porównać uzyskane skróty z tymi z ujawnionej bazy danych. Pozwala im to bardzo szybko złamać hasła.

Prawne wątpliwości przy korzystaniu z bazy haseł

Niektóre internetowe narzędzia do sprawdzania haseł oferują przeszukiwanie baz danych zawierających hasła, które wyciekły, aby sprawdzić, czy dane hasło się w nich znajduje lub czy jest podobne do hasła z bazy. Jest to przydatna funkcja, ale opiera się ona na danych uzyskanych w wyniku wycieków. Oprócz wyzwań technicznych związanych z integracją i aktualizacją takiej bazy danych w ramach aplikacji, pojawiłyby się również kwestie prawne, ponieważ korzystanie z tych baz danych mogłoby zostać uznane za przetwarzanie skradzionych danych.

Podsumowanie

Aplikacja FantomApp pozwala sprawdzić, czy hasło ma odpowiednią siłę i wyświetla ocenę szacującą, ile czasu zajęłoby hakerom jego odgadnięcie. Czas ten opiera się na założeniu, że hasło jest zbliżone do losowego ciągu znaków, co oznacza, że haker nie byłby w stanie go łatwo odgadnąć. Oczywiście kalkulator poda ten sam szacunkowy czas zarówno dla hasła „TwojeHasło123!”, jak i „xB#3Tt!bYak\$c2”, ponieważ oba spełniają te same kryteria (długość, wielkie litery, małe litery, cyfry i znaki specjalne). Należy zachować ostrożność przy interpretacji wyświetlanego czasu – odnosi się on wyłącznie do haseł przypominających drugi rodzaj ciągu znaków.

To narzędzie działa lokalnie na telefonie lub w przeglądarce i żadne dane nie są nigdy wysyłane na zewnątrz. Dzięki temu użytkownik może bezpiecznie testować swoje hasła, a jednocześnie poznawać najlepsze praktyki dotyczące tworzenia silnych haseł. Powodem, dla

którego nie wspomniano o menedżerach haseł, jest pierwotna grupa docelowa aplikacji FantomApp. Chociaż menedżery haseł są niezbędne dla zachowania dobrej higieny cyfrowej, mogą wydawać się skomplikowane dla dzieci w wieku od 10 do 15 lat, a wybór silnego hasła jest już ważnym pierwszym krokiem. Warto rozważyć również włączenie uwierzytelniania dwuskładnikowego.