UNIWERSYTET WARSZAWSKI

Dział Organizacji Zasobów Informacyjnych

DOZI-020-15/2020 Warszawa, dnia 19 marca 2020 roku

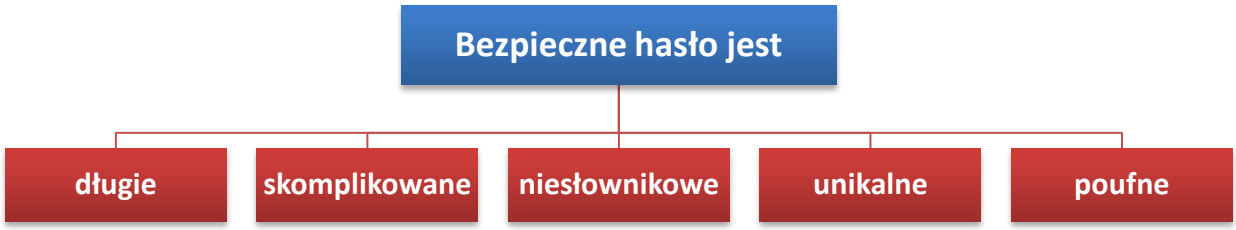
Szanowni Państwo,

w związku z *zarządzeniem nr 57 Rektora Uniwersytetu Warszawskiego z dnia 17 marca 2020 r. w sprawie czasowego ograniczenia obowiązku pracy na terenie uczelni w związku z zapobieganiem rozprzestrzenianiu się wirusa COVID-19* zdecydowana większość pracowników administracji centralnej, a także wydziałów i innych jednostek organizacyjnych pracuje w trybie zdalnym z własnego domu. Ten szczególny rodzaj pracy wymaga od każdego z nas szczególnej troski o bezpieczeństwo danych osobowych oraz innych poufnych informacji, które przetwarzamy w imieniu Uniwersytetu Warszawskiego. Poniższy poradnik ma na celu zwrócenie Państwa uwagi na kilka kluczowych działań, których wdrożenie pomoże Państwu zwiększyć poziom bezpieczeństwa informacji.

UNIWERSYTET WARSZAWSKI
Dział Organizacji Zasobów Informacyjnych
kierownik
mgr Dominik Ferenc

ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
tel.: 22 55 22 042
e-mail: iod@adm.uw.edu.pl

1. Jak tworzyć bezpieczne hasła?



Długie

Długie hasło składa się z co najmniej **8 znaków**, chociaż obecnie coraz częściej zachęca się do tworzenia haseł składających się z co najmniej **16 znaków**. Im dłuższe hasło, tym więcej czasu i środków trzeba poświęcić na jego złamanie metodą „brute force", dlatego długie hasła mogą skutecznie zniechęcić potencjalnego włamywacza.

Skomplikowane

Skomplikowane hasło zawiera **małe i wielkie litery, cyfry znaki specjalne**, a także **spacje**. Należy również pamiętać o tym, żeby unikać powtarzania pojedynczych znaków (np. **HXGqq96ZQ**) oraz pisania znaków w alfabetycznej kolejności (np. **abcdHGq96Z1234**).

Niesłownikowe

Jedynym z podstawowych zabiegów stosowanych przy łamaniu haseł metodą „brute force" jest wpisywanie nazw własnych i wyrazów słownikowych. Można się przed tym zabezpieczyć tworząc **hasła losowe lub pseudolosowe**, ale także w odpowiedni sposób kodując łatwe do zapamiętania słowa, np. zdanie „**Ala ma kota**" można zamienić na „**Al@ Ma K0+a**".

Unikalne

Wszystkie tworzone hasła powinny być unikalne, tzn. do każdej usługi www należy używać całkiem innego hasła. Należy przy tym unikać tworzenia haseł z dodatkami łatwymi do odgadnięcia, ponieważ wyciek jednego hasła można ułatwić odgadnięcie pozostałych, np. **HXGqq96ZQ-USOS**; **HXGqq96ZQ-SAP**; **HXGqq96ZQ-IRK**

Poufne

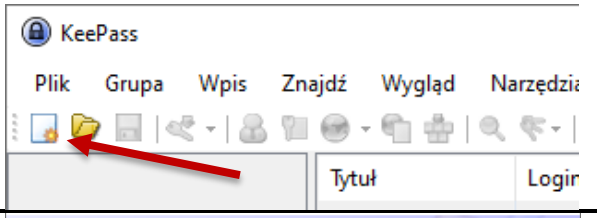
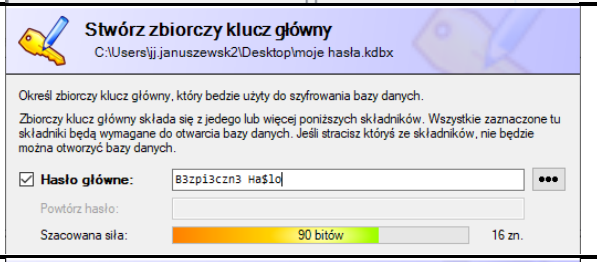
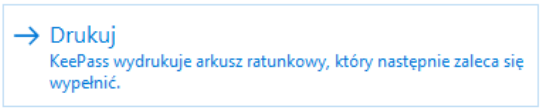
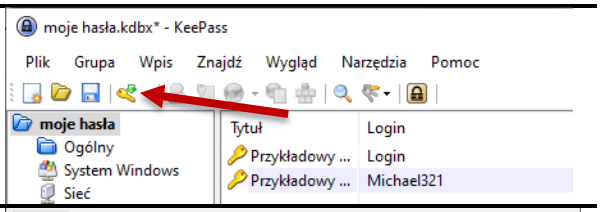
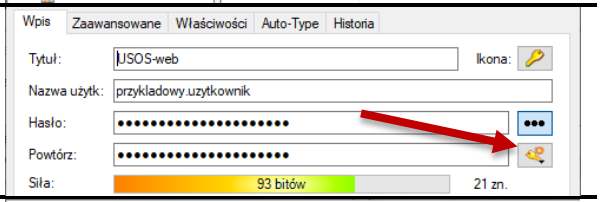
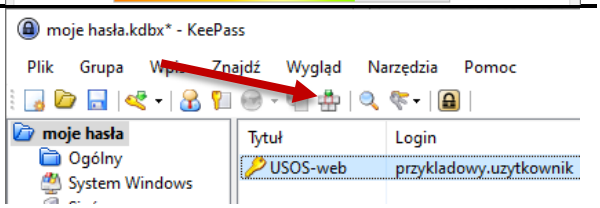
Nawet 32-znakowe, skomplikowane, losowe i unikalne hasło nie będzie stanowiło żadnego zabezpieczenia, jeżeli nie będzie ono przechowywane w bezpieczny sposób. Nigdy nie zapisuj swoich haseł **otwartym tekstem** w notesie, na karteczce przyklejonej do laptopa ani szczególnie **w pamięci przeglądarki internetowej**.

Hasła należy przechowywać jedynie **w formie zaszyfrowanej**, np. w **menedżerze haseł**

2. Jak bezpiecznie przechowywać hasła?

Najbezpieczniejszym narzędziem do przechowywania haseł są tzw. menedżery haseł, czyli specjalne programy, które pozwalają na **utworzenie zaszyfrowanej bazy** danych zawierającą hasła oraz związane z nimi loginy, adresy URL oraz inne przydatne informacje. Najpopularniejszym darmowym menedżerem haseł jest KeePass (keepass.info/download), dostępny również w wersji alternatywnej KeePassXC (keepassxc.org/download).

Zarządzanie hasłami w KeePass:

Krok 1. – utwórz nową bazę haseł	
Krok 2. – utwórz bezpieczne hasło główne	
Krok 3. – nazwij bazę haseł i zostaw pozostałe ustawienia domyślne	
Krok 4. – wydruk arkusz ratunkowy i zachowaj go w bezpiecznym miejscu	
Krok 5. – utwórz nowe hasło w bazie	
Krok 6. – bezpieczne hasło możesz łatwo utworzyć wbudowanym generatorem	
Krok 7. – mając **<u>otwartą w tle</u>** przeglądarkę z ekranem logowania, możesz użyć automatycznego wpisania hasła	

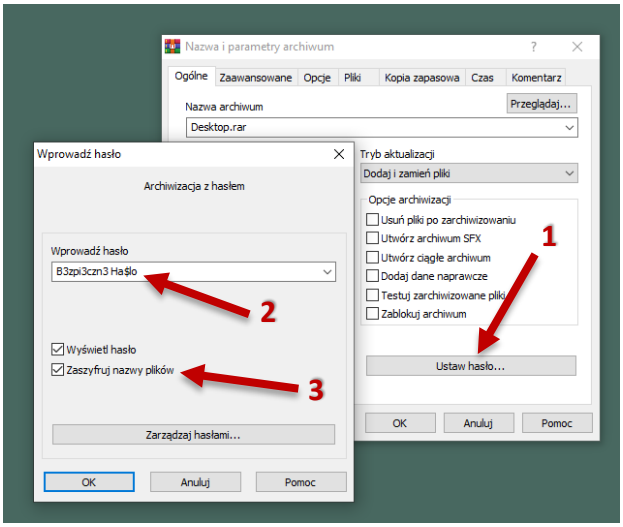
3. Jak zabezpieczyć pliki z poufnymi informacjami?

Pliki zawierające dane osobowe lub inne poufne informacje powinny być **zaszyfrowane** przed ich przesłaniem drogą mailową. Działanie takie pozwoli uniknąć ujawnienia ich treści w przypadku przypadkowego wysłania ich do niewłaściwego odbiorcy lub włamania na skrzynkę pocztową. Hasło do odblokowania plików należy zawsze podawać **inną formą komunikacji**, np. wysyłając SMS, dzwoniąc lub uprzednio ustalając wspólne hasło.

Szyfrowanie archiwum plików

Najprostszą metodą zabezpieczenia poufnych plików przed niepowołanymi osobami jest umieszczenie ich przed wysłaniem w archiwum plików (zip, rar, tar, 7z, itp.) **zabezpieczonym hasłem**. Opcja ta jest dostępna np. w programach WinRAR, WinZip, 7-Zip.

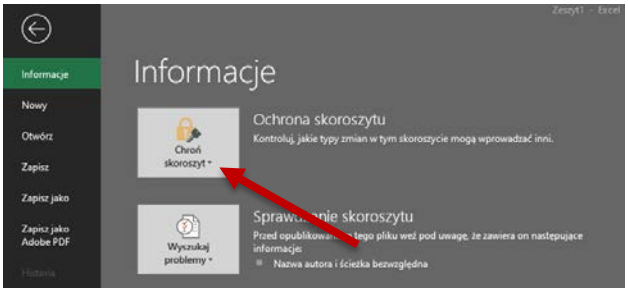
Jeżeli nazwy plików również mogą zawierać poufne informacje zaznacz opcję „**zaszyfruj nazwy plików**”.



Szyfrowanie plików MS Office

Programy z pakietu MS Office również umożliwiają zabezpieczanie poufnych plików hasłem. Opcja ta jest dostępna w zakładce: **Plik → Informacje**.

W zależności od programu nazwa opcji może nieznacznie się różnić np. „Ochrona dokumentu”, „Ochrona skoroszytu”, itp.



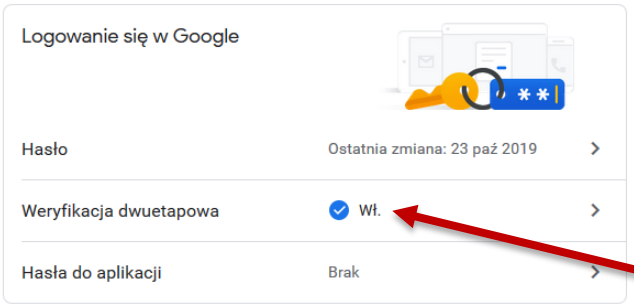
Pamiętaj, że w większości przypadków odzyskanie hasła do zaszyfrowanego dokumentu jest **niemożliwe**. Dlatego należy zapisywać w bezpiecznym miejscu hasła używane do szyfrowania plików, a także zabezpieczać wysyłaną **kopię pliku**, a nie sam plik przechowywany na dysku.

4. Jak włączyć weryfikację dwuetapową (2FA) w Google?

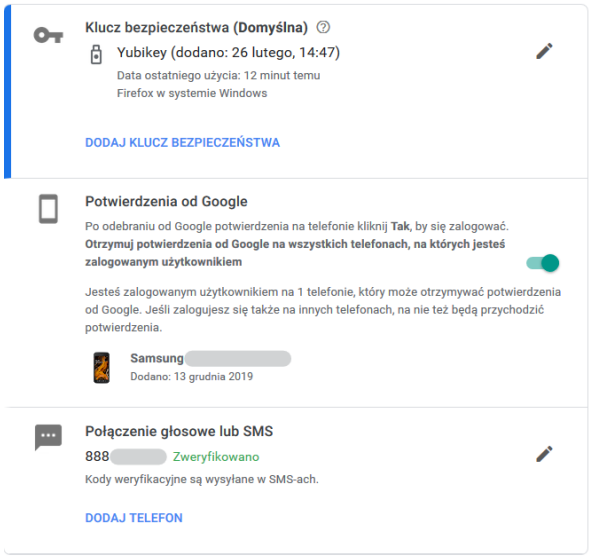
Bardzo często dane osobowe oraz inne poufne informacje są przetwarzane za pośrednictwem narzędzi Google w ramach usługi *G-Suite dla edukacji* wdrożonej na Uniwersytecie Warszawskim, np. Dysk Google, Formularze Google, Mapy Google, itp.

Należy pamiętać, że wszystkie informacje przetwarzane w usługach Google są w rzeczywistości przechowywane w serwerach tej firmy, a nie zasobach sieciowych UW. Oznacza to również, że dostęp do nich można uzyskać łącząc się spoza sieci UW bez korzystania z dodatkowych zabezpieczeń jak uniwersytecki VPN.

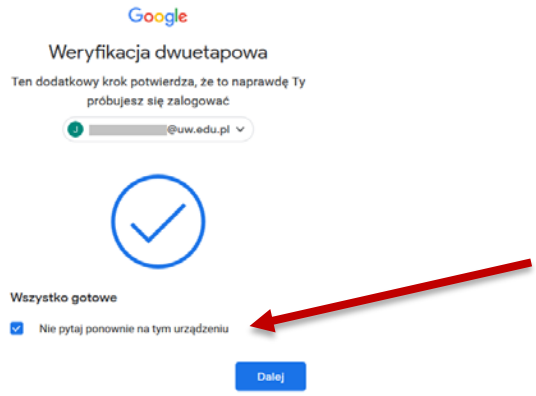
Najlepszą metodą zabezpieczenia konta Google przed nieuprawnionym dostępem jest włączenie weryfikacji dwuetapowej po zalogowaniu się na konto na stronie: https://account.google.com/security



Po uruchomieniu weryfikacji dwuetapowej, do zalogowania na konto Google za każdym razem będzie potrzebne nie tylko wprowadzenie hasła do konta, ale również potwierdzenie swojej tożsamości jedną ze skonfigurowanych opcji, jak zaufany telefon komórkowy, zewnętrzny token, połączenie głosowe lub wiadomość SMS lub aplikacja Google Authenticator.



W celu zwiększenia wygody korzystania z konta Google z włączoną weryfikacją dwuetapową, możliwe jest dodanie swojego komputera do listy urządzeń zaufanych podczas logowania. Komputer zostanie wówczas „zapamiętany” przez Google i nie będzie konieczne na nim każdorazowe korzystanie z drugiego etapu weryfikacji tożsamości.



Pamiętaj, że weryfikację dwuetapową możesz ustawić także w innych usługach internetowych, z których korzystasz: Microsoft, Facebook, Twitter, itp.

5. Przydatne linki

Powyższy poradnik uwzględnia tylko kilka kluczowych działań mających na celu zwiększenie bezpieczeństwa informacji przetwarzanych przez pracowników Uniwersytetu Warszawskiego podczas pracy zdalnej. Osoby chcące poszerzyć swoją wiedzę w tym zakresie powinny również zapoznać się z poniższymi artykułami, poradnikami i filmami:

Sprawdź czy Twoje dane wyciekły:

- https://haveibeenpwned.com/
- https://monitor.firefox.com/
- https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html

Bezpieczne hasła:

- https://techinfo.uodo.gov.pl/hasla-praktyczne-wskazowki-czy-naprawde-trzeba-zmienic-haslo-co-30-dni/
- https://uodo.gov.pl/pl/138/1285
- https://sekurak.pl/kompendium-bezpieczenstwa-hasel-atak-i-obrona/

Menedżery haseł:

- https://niebezpiecznik.pl/post/keepass-jak-zaczac-swoja-przygode-z-managerem-hasel/
- https://sekurak.pl/keepass-system-zarzadzania-haslami/
- https://trybawaryjny.pl/keepass-instalcja-obsluga/

Szyfrowanie plików:

- https://www.komputerswiat.pl/poradniki/programy/7-zip-jak-stworzyc-archiwum-na-haslo/ey3dz1t
- https://support.microsoft.com/pl-pl/help/4026312/windows-10-how-to-encrypt-a-file

Weryfikacja dwuetapowa

- https://support.google.com/accounts/answer/185839
- https://support.microsoft.com/pl-pl/help/12408/microsoft-account-how-to-use-two-step-verification
- https://www.facebook.com/help/148233965247823/
- https://help.twitter.com/en/managing-your-account/two-factor-authentication

Opracował: *Jacek Januszewski*

marzec 2020 r.