UWOLNIJ UMYSŁ

Wytyczne do pracy zdalnej

UNIWERSYTET ŁÓDZKI

www.uni.lodz.pl

Wytyczne dzielimy na dwa obszary:

Prywatne łącze internetowe

Korzystaj jedynie z zaufanych sieci.

Unikaj publicznych sieci, które są ogólnodostępne i niezabezpieczone hasłem. Wbrew pozorom nie ma nic za darmo. W takich sieciach może odbywać się skanowanie całego ruchu, a co za tym idzie łatwo jest przechwycić np. hasła czy kody bankowe.

Zabezpiecz dostępowe urządzenie sieciowe.

Zweryfikuj czy nie korzystasz z domyślnego hasła logowania do Swojego routera i bezwzględnie je zmień. Zalecane jest aby hasło zawierało min. jedną dużą literę, jedną małą literę, jedną cyfrę i jeden znak specjalny oraz żeby miało minimalną długość 8 znaków.

Zabezpieczenie sieci.

Ustaw hasło do sieci bezprzewodowej WIFi. Sprawdź czy w Swojej sieci bezprzewodowej WiFi masz ustawione hasło i czy wymaga ona logowania. Jeśli nie, ustaw odpowiedni poziom zabezpieczeń logowania do sieci WiFi np. WPA2 z szyfrowaniem AES i bezpieczne hasło. Zalecane jest aby hasło zawierało min. jedną dużą literę, jedną małą literę, jedną cyfrę i jeden znak specjalny oraz żeby miało minimalną długość 8 znaków.

Do pracy potrzebujesz odpowiednich parametrów sieci.

- **Szybkość Twojej sieci.**

Do pracy zdalnej i korzystania ze spotkań audio-wideo np. w programie Microsoft Teams w konfiguracji jeden-na-jeden (rozmowa audio-wideo pomiędzy dwoma uczestnikami) rekomendujemy, aby minimalna przepustowość sieci w każdym kierunku miała minimum 4Mb/s. Oznacza to, że zarówno nadawanie jak i odbiór (download i upload) nie powinien być mniejszy niż 4Mb/s.

W praktyce większość domowych sieci kablowych i światłowodowych spełnia powyższy warunek. Dla spotkań wieloosobowych czy konferencji audio-wideo, wymagana jest sieć o proporcjonalnie wyższych parametrach. Czym więcej uczestników spotkania audio-wideo, tym wyższa powinna być przepustowość sieci w obu kierunkach.

Aby sprawdzić przepustowość Twojej sieci, możesz skorzystać z testu łącza internetowego pod adresem www.speedtest.net *(kliknij)***. Sugerujemy, aby test łącza internetowego wykonywany był podłączonym po kablu komputerem lub laptopem, gdyż połączenia bezprzewodowe mogą generować błędne wyniki pomiaru.**

- **Stabilność Twojej sieci.**

Poprawna praca sieci oprócz odpowiedniej przepustowości wymaga także stabilności. Każdy wysyłany czy odbierany pakiet informacji w sieci jest potwierdzany „po drugiej stronie". W zadanym przedziale czasowym wysyłana jest odpowiednia ilość pakietów informacji, na które to odpowiedzi wymagają także pewnego określonego czasu. Średnia czasów odpowiedzi na przesłane pakiety

jest czasem opóźnienia sieci. Im sieć jest stabilniejsza tym średnia czasów odpowiedzi, opóźnienia sieci, jest krótsza. Opóźnienie sieci możesz zweryfikować korzystając z testu łącza internetowego pod adresem **www.speedtest.net.** Najstabilniejszymi łączami są łącza kablowe i światłowodowe (tzw. łącza stałe), w których opóźnienia nie przekraczają 1-2ms. Im stabilniejsza sieć i krótsze czasy odpowiedzi tym przekaz audio-wideo będzie miał lepszą jakość i mniejsze opóźnienia.

- **Dlaczego sieć komórkowa to nie jest najlepszy pomysł?**

Ze względu na przepustowość oraz stabilność, a co za tym idzie wyższą przepustowość i mniejsze opóźnienia przy łączach stałych, zalecamy wybór właśnie połączeń kablowych lub WiFi. Sieć komórkowa, w zależności od typu nadajnika i ilości połączeń do niego, może nie zapewniać odpowiedniej przepustowości łącza i może wprowadzać większe opóźnienia, co będzie powodować problemy z transmisjami audio-wideo.

Jeśli nie masz innego wyboru i musisz skorzystać z sieci komórkowej, sugerujemy przy gorszych parametrach sieci na wyłączanie transmisji wideo aby poprawić jakość transmisji audio. Jakość swojej sieci komórkowej, możesz także sprawdzić korzystając z testu łącza internetowego pod adresem **www.speedtest.net**

Prywatny komputer

Do pracy zdalnej rekomendujemy urządzenia z zainstalowanym systemem operacyjnym Windows 10 (Home) lub Windows 10 Pro w wersjach 1909, 2004 oraz 20H2 (stan na listopad 2020). Wersję systemu operacyjnego Windows 10 możesz sprawdzić otwierając: „Ustawienia” -> „System” -> „Informacje”.

Dbaj o aktualność Twojego systemu operacyjnego.

Dla zapewnienia stabilnej i bezpiecznej pracy oraz dostępu do nowych funkcji, system operacyjny wymaga poprawek i aktualizacji. Windows 10 posiada wbudowaną funkcjonalność aktualizacji automatycznych, które wdrażane są np. przy okazji wyłączania i włączania komputera. Sugerujemy wdrażanie i aktualizowanie swoich urządzeń na bieżąco i nieodkładanie wymaganych aktualizacji w czasie.

Dbaj o aktualność całego oprogramowania.

- Większość markowych komputerów osobistych oraz laptopów oprócz aktualizacji systemu operacyjnego posiada także oprogramowanie pozwalające na aktualizację zabezpieczeń i stabilności oprogramowania układowego (tj. firmware'ów) poszczególnych komponentów komputera czy laptopa oraz sterowników tych podzespołów. W związku z bezpieczeństwem i stabilnością tychże podzespołów, zalecamy aby wykonywać także aktualizację firmware'ów i sterowników. Aktualizacja większości sterowników przeprowadzana jest również przez sam system operacyjny Windows 10 podczas aktualizacji systemu operacyjnego.

- Jeśli korzystasz z przeglądarki innej niż wbudowana w Windows 10 przeglądarka tj. Microsoft Edge (Chromium), która aktualizowana jest wraz z systemem operacyjnym Windows 10, ze względów bezpieczeństwa i stabilności pracy aktualizuj także swoją ulubioną przeglądarkę internetową. Aktualnie dostępne przeglądarki internetowe w większości posiadają już wbudowane moduły automatycznych aktualizacji.

Rekomendowane przeglądarki do pracy zdalnej to: Microsoft Edge (Chromium), Google Chrome oraz Mozilla Firefox.

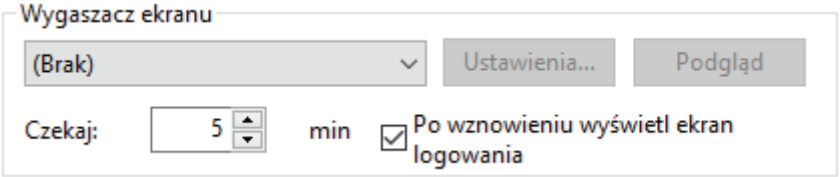
Zabezpiecz komputer hasłem.

Dbając o bezpieczeństwo Twojego komputera czy laptopa a przede wszystkim znajdujących się na nim danych przed niepowołanym dostępem, koniecznie zabezpiecz logowanie do swojego komputera bezpiecznym hasłem. Zalecane jest aby hasło zawierało min. jedną dużą literę, jedną małą literę, jedną cyfrę i jeden znak specjalny oraz żeby miało minimalną długość 8 znaków.

- **Pamiętaj aby użyte hasła różniły się miedzy sobą**, a przede wszystkim żeby nie pokrywały się z hasłami jakich używasz korzystając z systemów i programów Uniwersytetu Łódzkiego czy innych dostępnych dla Ciebie usług.

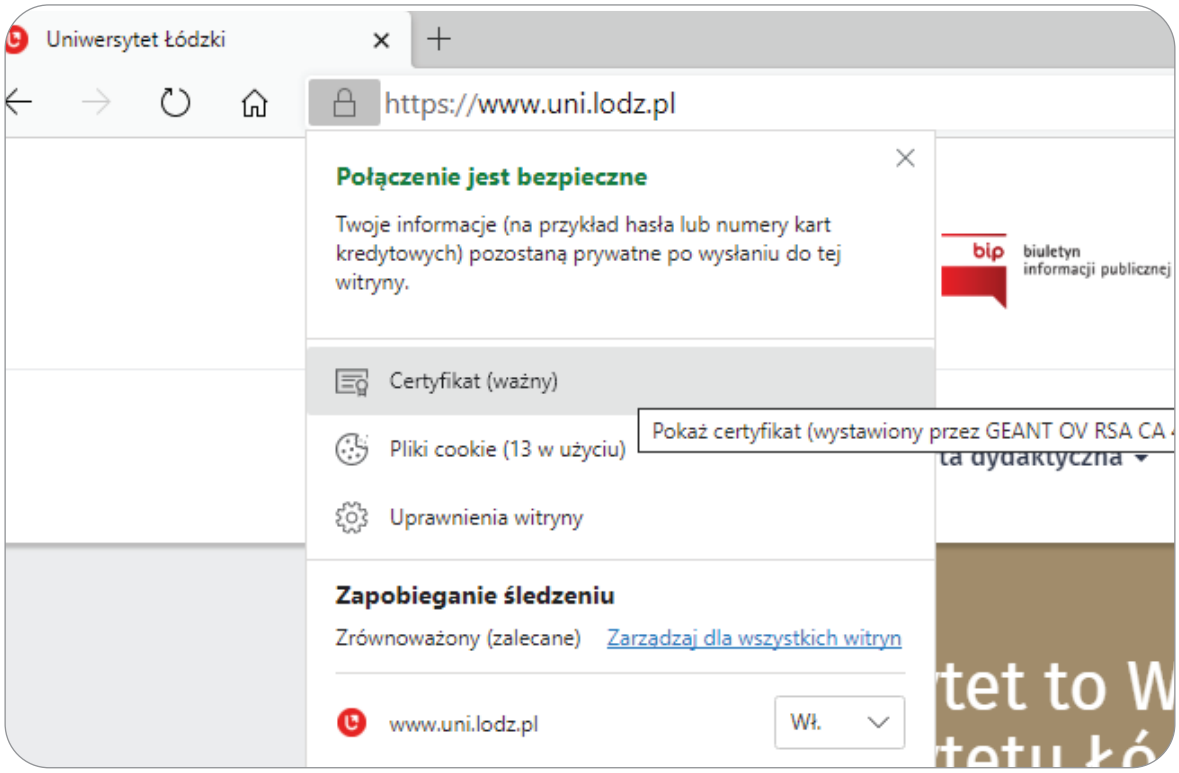
- **Dla zapewnienia bezpieczeństwa i nieautoryzowanego dostępu, pamiętaj o zablokowaniu Twojego komputera nawet jeśli robisz przerwę w pracy i odchodzisz na chwilę od urządzenia**. Aby zablokować komputer wystarczy wybrać na klawiaturze kombinację klawiszy „WIN” (symbol Windows'a obok lewego klawisza „ALT”) + „L”. Zablokowany w ten sposób komputer po Twoim powrocie do pracy będzie ponownie wymagał wprowadzenia ustawionego hasła.

- **Zalecamy również włączenie automatycznego blokowania komputera po czasie bezczynności urządzenia**, w razie gdybyś odszedł od komputera i zapomniał go zablokować ręcznie. Aby uruchomić automatyczne blokowanie w Windows 10 wejdź w: „Ustawienia” -> „Personalizacja” -> „Ekran blokady” -> „Ustawienia wygaszacza ekranu” i skonfiguruj wszystkie opcje jak na poniższym przykładzie.

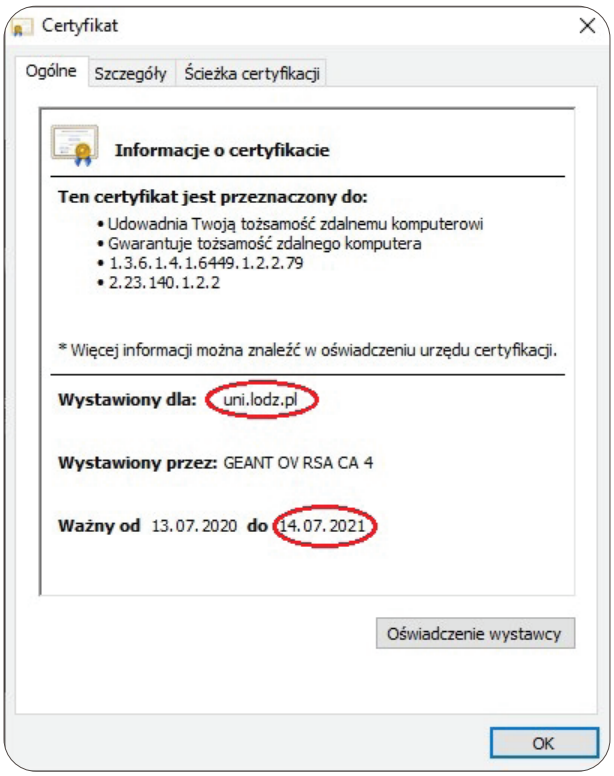


Podczas korzystania z przeglądarki internetowej pamiętaj aby ze względów bezpieczeństwa nie wchodzić na strony, których nie znasz lub wydają Ci się podejrzane.

Aktualnie większość witryn internetowych jest szyfrowana i zabezpieczona certyfikatem, co uwidocznione jest przez np. symbol zamkniętej kłódki (również w kolorze zielonym) znajdującej się na początku paska adresu witryny internetowej. Klikając na tę kłódkę możesz sprawdzić certyfikat odwiedzanej strony.



Po wyświetleniu certyfikatu możesz sprawdzić jego ważność i dla jakiej witryny został on wystawiony. Nazwa bądź końcówka nazwy wystawionego certyfikatu powinna być zgodna z nazwą bądź końcówką witryny którą odwiedzamy.



Pamiętaj także aby nie pobierać plików z nieznanych, a przede wszystkim niezabezpieczonych i niecertyfikowanych stron internetowych.

Uważaj również na przekierowania (linki) we wiadomościach poczty elektronicznej oraz ich załączniki.

Sprawdzaj nazwę domenową (końcówkę) wiadomości e-mail nadawcy i nie sugeruj się nazwą wyświetlaną. Przykładowo jeśli w nazwie nadawcy wiadomości e-mail wyświetlana jest nazwa „DHL Parcel" poszukaj w niej adresu e-mail nadawcy. Jeśli e-mail nadawcy to np. „dhl@parcel.com" , jest to wiadomość fałszywa, gdyż DHL używa z reguły końcówki „dhl.com" i nazwa powinna kończyć się właśnie taką domeną. Bądź uważny i dokładnie czytaj wszystkie informacje zanim cokolwiek klikniesz.

Jeśli w celach służbowych korzystasz z komputera przenośnego, dobrym pomysłem jest włączenie na nim szyfrowania dysku.

W związku z tym, że na Twoim urządzeniu mogą znajdować się poufne dane, w razie kradzieży lub zgubienia laptopa z zaszyfrowanym dyskiem, dostęp do takich danych będzie mocno utrudniony. Zabezpieczony wcześniej hasłem komputer nie pozwoli postronnej osobie na zalogowanie się do niego, a ewentualne wyjęcie i przełożenie dysku do innego urządzenia spowoduje, że dane znajdujące się na zaszyfrowanym dysku nie będą dostępne.

Instrukcję włączenia szyfrowania dysku zarówno dla Windows 10 (Home) jak i Windows 10 Pro znajdziesz na stronie **www.support.microsoft.com**

Dla zachowania bezpieczeństwa Twojego komputera oraz znajdujących się na nim danych zawsze używaj oprogramowania zabezpieczającego z aktywnym i aktualnym antywirusem.

W aktualnych wersjach Windows 10 wbudowanym i bezpłatnym narzędziem zabezpieczającym jest pakiet oprogramowania zwany „Zabezpieczenia Windows", w skład którego wchodzi min. antywirus „Microsoft Defender". „Zabezpieczenia Windows", którym jednym ze składników jest „Microsoft Defender", symbolizowane są ikoną białej tarczy w okolicach zegara na pasku zadań.

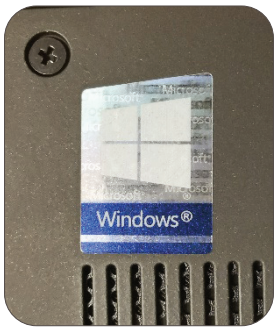
Jeśli oprogramowanie jest zaktualizowane i nie wymaga interwencji użytkownika ikona tarczy wygląda następująco:  .

Aktualne szczepionki i ustawienia zabezpieczeń pobierane są automatycznie w trakcie aktualizacji systemu operacyjnego Windows 10.

Abyś mógł bezpiecznie użytkować swój komputer pamiętaj, że wszystkie powyższe zabezpieczenia mogą nie wystarczyć.

Aby zapobiec wyciekowi poufnych danych z Twojego komputera, pamiętaj żeby używać wyłącznie legalnego oprogramowania zakupionego u sprawdzonego i autoryzowanego sprzedawcy. Nielegalne i pirackie kopie oprogramowania mogą zawierać w sobie programy lub fragmenty kodu, które przy połączeniu z siecią Internet mogą przekazywać dane z Twojego urządzenia, a antywirus może być spreparowany w ten sposób, aby nie wychwytywał niepożądanego działania takich programów.

Większość sprzedawanych obecnie komputerów stacjonarnych czy laptopów znanych marek jest fabrycznie wyposażona w oficjalny i w pełni legalny system operacyjny Windows 10, co powinno być potwierdzone naklejką znajdującą się na tyle, boku lub spodzie twojego komputera lub laptopa.



Ważne. Pamiętaj, że jako pracownikowi Uniwersytetu Łódzkiego, który używa swoich prywatnych urządzeń w celach służbowych (mogą być to zarówno komputer stacjonarny, laptop, tablet bądź smartfon), masz prawo do zainstalowania pakietu Microsoft Office, jego składników bądź aplikacji na maksymalnie 5 takich urządzeniach.