



AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole

I. Jak dużo dobrego w bezpieczeństwie niesie za sobą Windows 11 Pro i Edu

Windows 11 Pro lub Edu ma wiele zabezpieczeń, z których użytkownik nawet nie zdaje sobie sprawy. Na co dzień zabezpieczają go one przed atakami lub wyłudzeniami itp. Oto niektóre z nich, które na stałe są w systemie:

1. **BitLocker:** To narzędzie do szyfrowania całych dysków, które chroni dane przed nieautoryzowanym dostępem. BitLocker używa algorytmów szyfrowania, aby zabezpieczyć dane na dyskach twardych i przenośnych, takich jak pendrive'y.
2. **Windows Hello:** Umożliwia bezpieczne logowanie do urządzeń za pomocą biometrii, np. rozpoznawania twarzy, odcisku palca, lub kodu PIN. To znacznie zwiększa bezpieczeństwo w porównaniu do tradycyjnych haseł.
3. **Windows Defender:** Wbudowany program antywirusowy i antymalware, który chroni system przed wirusami, złośliwym oprogramowaniem i innymi zagrożeniami online; regularnie aktualizuje swoje definicje zagrożeń, aby zapewnić najnowszą ochronę.
4. **Hyper-V:** Technologia wirtualizacji, która pozwala na uruchamianie wielu systemów operacyjnych na jednym komputerze. Przydaje się do testowania oprogramowania w izolowanych środowiskach.
5. **Windows Sandbox:** Bezpieczne środowisko do uruchamiania nieznanych aplikacji i plików bez ryzyka dla głównego systemu. Po zamknięciu Sandbox wszystkie dane są usuwane, co zapewnia, że system pozostaje czysty.
6. **Microsoft Defender Application Guard:** Chroni przeglądarkę i aplikacje przed złośliwym oprogramowaniem, uruchamiając je w izolowanym kontenerze. Nawet jeśli aplikacja zostanie zainfekowana, nie wpłynie to na resztę systemu.
7. **Secured-core PCs:** Urządzenia te mają dodatkowe warstwy zabezpieczeń sprzętowych, które chronią przed zaawansowanymi atakami. Są one bardziej odporne na ataki typu firmware i inne zagrożenia na poziomie sprzętu.
8. **Microsoft Pluton Security Processor:** Nowy procesor bezpieczeństwa, który integruje się bezpośrednio z CPU, aby chronić wrażliwe dane, takie jak klucze szyfrowania, przed atakami fizycznymi i zdalnymi.
9. **Virtualization-Based Security (VBS):** Używa technologii wirtualizacji do ochrony krytycznych części systemu operacyjnego przed złośliwym oprogramowaniem. VBS tworzy izolowane środowisko, które utrudnia atakom dostęp do systemu.
10. **Hypervisor-Protected Code Integrity (HVCI):** Chroni przed atakami na jądro systemu operacyjnego, zapewniając, że tylko zaufany kod może być wykonywany.

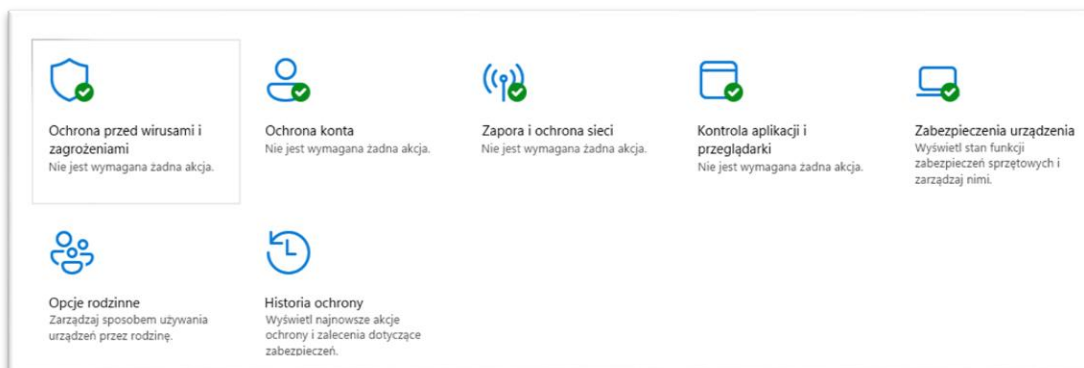
AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

11. **Windows Information Protection (WIP):** Pomaga chronić dane firmowe przed przypadkowym wyciekiem, umożliwiając kontrolę nad tym, które aplikacje mogą uzyskiwać dostęp do danych firmowych.
12. **Credential Guard:** Chroni poświadczenia użytkowników przed kradzieżą przez złośliwe oprogramowanie, izolując je w bezpiecznym środowisku.
13. **Advanced Threat Protection (ATP):** Zaawansowane narzędzie do wykrywania zagrożeń i reagowania na nie; monitoruje system w czasie rzeczywistym i analizuje podejrzane działania.
14. **Passkeys:** Umożliwia bezhasłowe logowanie, co zwiększa bezpieczeństwo i zmniejsza ryzyko ataków phishingowych. Passkeys są bardziej bezpieczne niż tradycyjne hasła, ponieważ nie są podatne na kradzież.

Domyślnie włączone zabezpieczenia w Windows 11 Pro to:

- Windows Defender: Ochrona przed wirusami i złośliwym oprogramowaniem jest włączona domyślnie.



- Secure Boot: Zapewnia, że komputer uruchamia się tylko z zaufanego oprogramowania.
- Windows Hello: Możliwość logowania za pomocą biometrii lub kodu PIN jest dostępna, ale wymaga konfiguracji.
- Firewall and Network Protection: Monitoruje i kontroluje ruch sieciowy.
- Credential Guard: Chroni poświadczenia użytkowników przed kradzieżą.

Zabezpieczenia, które można włączyć ręcznie:

BitLocker

- Otwórz Ustawienia.
- Przejdź do Aktualizacji i zabezpieczeń.
- Wybierz Szyfrowanie urządzenia.
- Kliknij „Włącz BitLocker” i postępuj zgodnie z instrukcjami na ekranie.



AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

Hyper-V

- Otwórz Panel sterowania.
- Przejdź do Programów.
- Kliknij „Włącz lub wyłącz funkcje systemu Windows”.
- Zaznacz opcję Hyper-V i kliknij OK.
- Uruchom ponownie komputer, aby zastosować zmiany.

Windows Sandbox

- Otwórz Panel sterowania.
- Przejdź do Programów.
- Kliknij „Włącz lub wyłącz funkcje systemu Windows”.
- Zaznacz opcję Windows Sandbox i kliknij OK.
- Uruchom ponownie komputer, aby zastosować zmiany.

Microsoft Defender Application Guard

- Otwórz Panel sterowania.
- Przejdź do Programów.
- Kliknij „Włącz lub wyłącz funkcje systemu Windows”.
- Zaznacz opcję „Microsoft Defender Application Guard” i kliknij OK.
- Uruchom ponownie komputer, aby zastosować zmiany.

Virtualization-Based Security (VBS) i Hypervisor-Protected Code Integrity (HVCI)

- Otwórz Ustawienia.
- Przejdź do Aktualizacji i zabezpieczeń.
- Wybierz Windows Security.
- Kliknij Device security.
- Wybierz Core isolation details.
- Włącz Memory integrity.

Windows Information Protection (WIP)

- Wymaga użycia narzędzi zarządzania IT, takich jak Microsoft Intune.
- Skonfiguruj zasady ochrony danych w Intune i przypisz je do odpowiednich urządzeń.

Advanced Threat Protection (ATP)

- Wymaga subskrypcji Microsoft Defender for Endpoint.
- Skonfiguruj ATP za pomocą portalu Microsoft 365 Defender.

AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

Passkeys

- Otwórz Ustawienia.
- Przejdź do Kont.
- Wybierz Opcje logowania.
- Wybierz Klucz bezpieczeństwa i postępuj zgodnie z instrukcjami na ekranie.

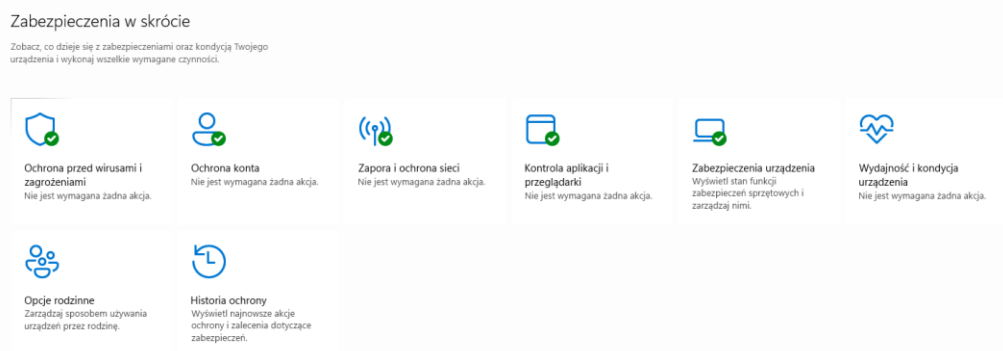
II. Jak włączyć zabezpieczenia przed niektórymi cyberatakami (np. przed ransomware)

Aby włączyć ochronę przed ransomware w Windows 11 Pro i Education, można skorzystać z funkcji Controlled Folder Access wbudowanej w Microsoft Defender.

Jak to zrobić – krok po kroku:

1. Otwórz Windows Security:

- Kliknij ikonę lupy na pasku zadań i wpisz „Windows Security”, a następnie wybierz aplikację z wyników wyszukiwania.



2. Przejdź do sekcji Virus & threat protection:

- W oknie Windows Security kliknij Virus & threat protection.

AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

Ustawienia ochrony przed wirusami i zagrożeniami

Nie jest wymagana żadna akcja.

[Zarządzaj ustawieniami](#)

Aktualizacje ochrony przed wirusami i zagrożeniami

Analiza zabezpieczeń jest aktualna.

Ostatnia aktualizacja: 27.09.2024 05:40

[Aktualizacje ochrony](#)

Ochrona przed oprogramowaniem ransomware

Nie jest wymagana żadna akcja.

[Zarządzaj ochroną przed oprogramowaniem ransomware](#)

3. Zarządzaj ochroną przed ransomware:

- Przewiń w dół do sekcji Ransomware protection i kliknij Manage ransomware protection.

4. Włącz Controlled Folder Access:

- Ustaw przełącznik Controlled folder access na „On”.

Ochrona przed oprogramowaniem ransomware

Chroń swoje pliki przed zagrożeniami, takimi jak oprogramowanie ransomware, i zobacz, jak przywrócić pliki w przypadku ataku.

Kontrolowany dostęp do folderu

Chroń pliki, foldery i obszary pamięci na urządzeniu przed nieautoryzowanymi zmianami wprowadzanymi przez nieprzyjazne aplikacje.

☒ Włączone

5. Dodaj chronione foldery:

- Kliknij „Protected folders”, aby dodać dodatkowe foldery, które chcesz chronić przed ransomware. Domyślnie chronione są foldery: Dokumenty, Obrazy, Filmy i Pulpit.

6. Zezwalaj aplikacjom na dostęp do chronionych folderów:

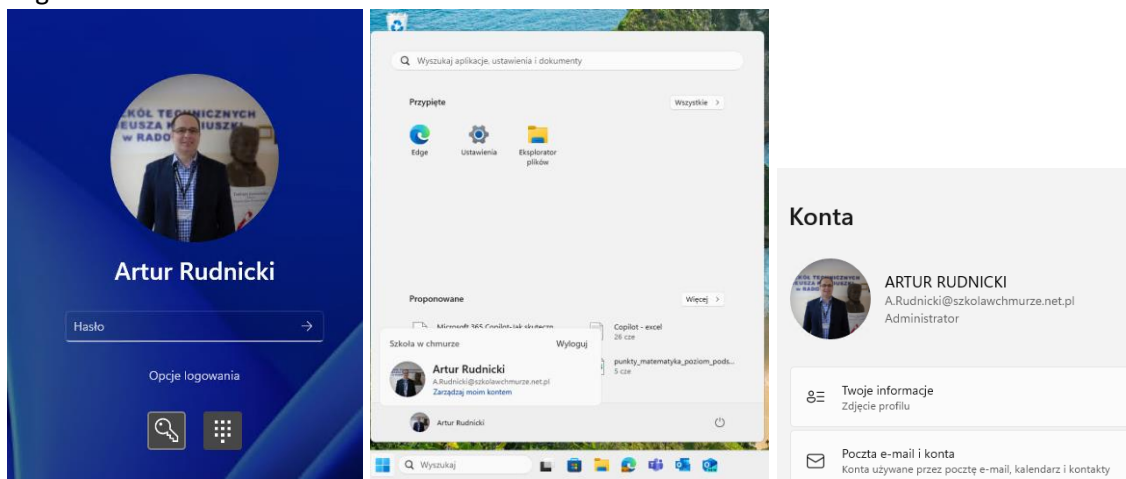
- Kliknij „Allow an app through Controlled folder access”, aby dodać aplikacje, którym ufasz i które mogą mieć dostęp do chronionych folderów. Możesz wybrać aplikacje z listy ostatnio zablokowanych lub przeglądać wszystkie aplikacje.

AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

III. Jak być zgodnym z RODO i tzw. ustawą Kamilka

Logowanie na konta szkolne w usłudze Microsoft 365.



IV. Jak w bezpieczny i wydajny sposób serfować po internecie

Microsoft Edge to nowoczesna przeglądarka internetowa oparta na silniku Chromium. Została zaprojektowana z myślą o szybkości, bezpieczeństwie i wydajności. Oferuje wiele unikalnych funkcji, takich jak:

- Copilot – asystent AI, który pomaga w przeglądaniu, odpowiada na pytania i oferuje sugestie,
- Vertical Tabs – umożliwia lepszą organizację kart, przenosząc je na bok ekranu,
- narzędzia do nauki.

Microsoft Edge oferuje wiele zaawansowanych zabezpieczeń, które pomagają chronić użytkowników podczas przeglądania internetu. Oto niektóre z nich:

Microsoft Defender SmartScreen

Ochrona przed phishingiem i złośliwym oprogramowaniem: SmartScreen blokuje podejrzane strony internetowe i pliki do pobrania, które mogą zawierać złośliwe oprogramowanie.

Password Monitor

Monitorowanie haseł: Sprawdza zapisane hasła pod kątem wycieków danych i informuje użytkownika, jeśli któreś z haseł jest zagrożone.

Edge Secure Network

Wbudowany VPN: Chroni połączenie sieciowe, ukrywając lokalizację i zabezpieczając dane przed dostępem osób trzecich.

AKADEMIA AI DLA EDUKACJI

Windows 11 Pro w Edukacji. Ochrona danych i bezpieczeństwo w szkole.

Enhanced Security Mode

Zwiększona ochrona: Wyłącza kompilację JavaScript JIT i włącza dodatkowe zabezpieczenia systemu operacyjnego, takie jak Hardware-enforced Stack Protection i Arbitrary Code Guard.

Tracking Prevention

Zapobieganie śledzeniu: Blokuje skrypty śledzące, które zbierają dane o użytkowniku, oferując trzy poziomy ochrony: Basic, Balanced i Strict.

Typo Protection

Ochrona przed literówkami: Ostrzega użytkownika, jeśli wpisze błędny adres URL, który może prowadzić do złośliwej strony.

Password Generator

Generowanie silnych haseł: Pomaga tworzyć silne i unikalne hasła podczas rejestracji na nowych stronach.

Kids Mode

Tryb dla dzieci: Oferuje bezpieczne środowisko przeglądania dla dzieci, z filtrowaniem treści i kontrolą rodzicielską.

Sandboxing

Izolacja procesów: Każda karta w przeglądarce działa w izolowanym środowisku, co minimalizuje ryzyko, że złośliwe oprogramowanie wpłynie na cały system.

V. W jaki sposób poprosić o zdalną pomoc w przypadku problemów

Aby poprosić o zdalną pomoc w Windows 11 Pro i Education, możesz skorzystać z funkcji Quick Assist.

Oto, jak to zrobić:

1. Otwórz Quick Assist:

- Naciśnij Ctrl + Windows + Q lub wpisz „Quick Assist” w polu wyszukiwania na pasku zadań i wybierz aplikację.

2. Uzyskaj pomoc:

- Kliknij „Uzyskaj pomoc”.
- Zaloguj się na swoje konto Microsoft.
- Skopiuj kod zabezpieczający i wyślij go do osoby, która ma Ci pomóc.

3. Osoba pomagająca:

- Otwiera Quick Assist, wybiera „Pomóż komuś” i wprowadza kod zabezpieczający.
- Po zatwierdzeniu kodu osoba pomagająca może zobaczyć Twój ekran i poprosić o kontrolę nad Twoim komputerem.

