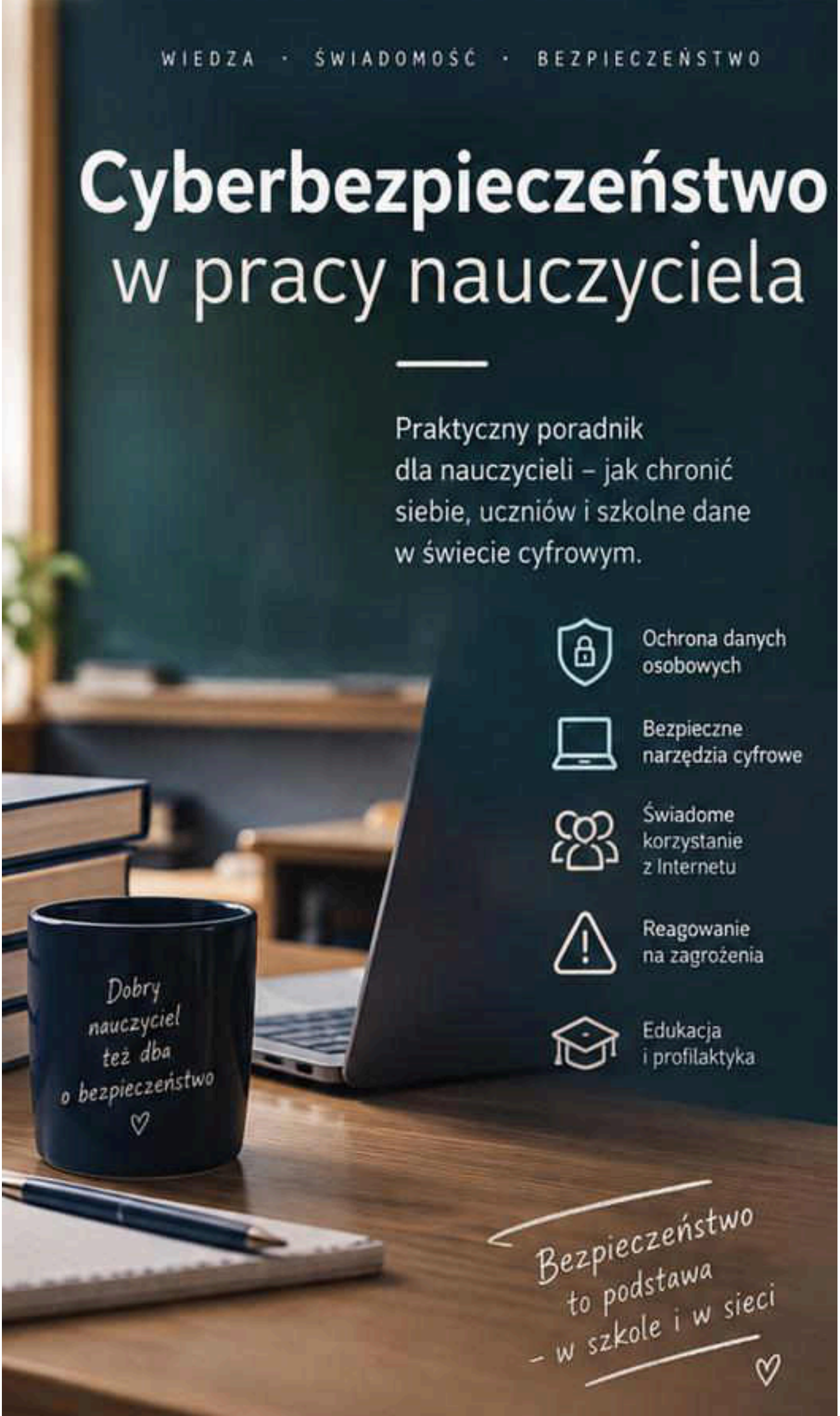

WIEDZA · ŚWIADOMOŚĆ · BEZPIECZEŃSTWO
Cyberbezpieczeństwo
w pracy nauczyciela
Praktyczny poradnik dla nauczycieli – jak chronić siebie, uczniów i szkolne dane w świecie cyfrowym.
Ochrona danych osobowych
Bezpieczne narzędzia cyfrowe
Świadome korzystanie z Internetu
Reagowanie na zagrożenia
Edukacja i profilaktyka
Dobry nauczyciel też dba o bezpieczeństwo
Bezpieczeństwo to podstawa – w szkole i w sieci

# Cyberbezpieczeństwo w pracy nauczyciela

Autorzy:

**Piotr Prach**

**Dariusz Kowal**

**Krzysztof Ryś**

**Kacper Pawlus**

**Piotr Rabich**

**Miłosz Szczygieł**

Recenzja:

**Doktor Nauk o Bezpieczeństwie Dominik Boratyn**

**Instytut Nauk o Polityce i Bezpieczeństwie Uniwersytetu Rzeszowskiego**

**Wydawca:**

Inżynieria Bezpieczeństwa strona: multisafety.pl

Koło Naukowe Mechatron-SEP Wydział Nauk Ścisłych i Technicznych
Uniwersytet Rzeszowski ul. Pigonia 1, 35-310 Rzeszów
Koło Studentów i Absolwentów przy UR Stowarzyszenie Elektryków Polskich Oddział Rzeszowski Ul. Kopernika 1 35-959 Rzeszów

ISBN 978-83-952298-4-8

Rok wydania: 2026

# Spis treści

**Rozdział 1. Ukrywanie życia prywatnego w mediach społecznościowych ..... 4**
Jakie informacje warto chronić? ..... 4
Sprawdzenie obecnej widoczności profilu ..... 4
Facebook - ograniczenie widoczności prywatnego profilu ..... 5
Instagram - konto prywatne i kontrola obserwujących ..... 7
TikTok - ograniczenie dostępu do filmów ..... 10
Nawyki pomagające oddzielić życie prywatne od pracy ..... 12
**Rozdział 2. Weryfikacja wycieków danych ..... 14**
Na czym polegają wycieki danych? ..... 14
Do wycieku poufnych informacji może dojść z kilku głównych powodów: ..... 14
Dlaczego to takie ważne w pracy nauczyciela? ..... 15
Jak weryfikować, czy nasze dane wyciekły? ..... 15
Co zrobić, gdy odkryjemy, że nasze dane wyciekły? ..... 18
**Rozdział 3. Jak nie dać się złapać na phishing ..... 19**
Jakie najczęściej nauczyciel może dostawać maile od cyberprzestępców? ..... 19
Jak rozpoznać próbę oszustwa? ..... 19
Zasady bezpieczeństwa ..... 20
Co zrobić w przypadku kliknięcia w złośliwy link? ..... 20
Pułapki przy nieznanych linkach ..... 21
**Rozdział 4. Tworzenie haseł, zarządzanie hasłami i weryfikacja dwuetapowa ..... 27**
Dlaczego tradycyjne podejście do haseł już nie wystarcza? ..... 27
Jak tworzyć pancerne hasła, które łatwo zapamiętać? ..... 27
Efekt domina – dlaczego każde konto musi mieć inne hasło? ..... 28
Menedżery haseł – osobisty cyfrowy sejf ..... 29
Dlaczego zapisywanie haseł w przeglądarce na szkolnym komputerze to pułapka? ..... 29
Sprawdzone i bezpieczny menedżer haseł ..... 29
Weryfikacja dwuetapowa (2FA / MFA) – tarcza na wypadek kradzieży hasła ..... 30
Jakie metody weryfikacji dwuetapowej są najbezpieczniejsze? ..... 31
Polecane aplikacje do weryfikacji dwuetapowej (2FA) ..... 31
Polityka bezpieczeństwa haseł w pracy – podsumowanie organizacyjne ..... 31

**Rozdział 5. Kanały komunikacji z uczniami, rodzicami oraz pracownikami. ..... 33**
Dlaczego komunikatory na social mediach są złe w pracy nauczyciela? ..... 33
**Rozdział 6. Deepfake i pułapki w AI ..... 34**
Czym jest technologia Deepfake i jak zmienia postrzeganie prawdy w sieci? ..... 34
Najczęstsze zagrożenia związane z Deepfake w środowisku szkolnym ..... 34
Jak rozpoznać materiał Deepfake? ..... 35
Narzędzia do weryfikacji, czy materiał to Deepfake lub wytwór AI ..... 35
Pułapki AI – jakich danych bezwzględnie NIE należy wprowadzać do czatbotów? ..... 37
Czarna lista danych – czego nie wolno wpisywać i wgrywać do AI: ..... 37
Pułapka „halucynacji AI" w materiałach edukacyjnych ..... 37
Jak bezpiecznie korzystać ze sztucznej inteligencji? ..... 38
**Rozdział 7. Bezpieczeństwo fizycznych urządzeń ..... 39**
Zabezpieczenie telefonu komórkowego ..... 39
Zabezpieczenie komputera ..... 40
Zagrożenia fizyczne: Nieznane nośniki USB ..... 42
**Rozdział 8. Co zrobić po włamaniu na E-dziennik lub maila służbowego? ..... 43**
Kogo powiadomić i dlaczego to takie ważne? ..... 43
**Rozdział 9. Jak uniknąć złośliwego oprogramowania ..... 45**
Czym jest złośliwe oprogramowanie? ..... 45
Podejrzane pliki i załączniki ..... 45
Sprawdzanie linku w VirusTotal ..... 47
Sprawdzanie pliku w VirusTotal ..... 47
Antywirus i ochrona w Windows 11 ..... 48
Nawyki ograniczające ryzyko ..... 49
**Rozdział 10. Zabezpieczanie dowodów cyfrowych ..... 50**
Jak poprawnie wykonywać zrzuty ekranu ..... 51
Metody zapisu zrzutów ekranu - komputery z systemem Windows: ..... 52
Metody zapisu zrzutów ekranu - Urządzenia mobilne (smartfony i tablety): ..... 52
Metody nagrywania ekranu - Urządzenia mobilne (smartfony i tablety) – opcje wbudowane. ..... 52
Metody nagrywania ekranu - komputery z systemem Windows. ..... 53
**Rozdział 11. Zgłaszanie incydentów ..... 54**

Wewnątrz struktur szkolnych i środowiska ucznia. ..... 54
Instytucje i organizacje specjalistyczne. ..... 54
Administratorzy platform i serwisów społecznościowych ..... 55
Organy ścigania i wymiar sprawiedliwości ..... 55
**Rozdział 12. Aspekty prawne i tarcza ochronna nauczyciela ..... 56**
Dlaczego mit „uczniowi nic nie można zrobić" to niebezpieczna fikcja? ..... 56
Tarcza funkcjonariusza publicznego – jak prawo chroni nauczyciela? ..... 56
Wykorzystanie wizerunku nauczyciela, memy, Deepfake i cyberprzemoc – co grozi uczniom? ..... 57
Groźby w sieci i fałszywe alarmy – kiedy „internetowy challenge" kończy się aresztem? 58
„Przecież jestem nieletni!" – jak w rzeczywistości wygląda odpowiedzialność ze względu na wiek? ..... 60
Gdzie kończą się uprawnienia nauczyciela, a kiedy działa obrona konieczna? ..... 61
Co zrobić krok po kroku, gdy padniesz ofiarą ataku w sieci lub w szkole? ..... 61

# Rozdział 1. Ukrywanie życia prywatnego w mediach społecznościowych

Media społecznościowe pozwalają utrzymywać kontakt z bliskimi, dzielić się zainteresowaniami i publikować wspomnienia. Jednocześnie mogą udostępniać informacje o naszym życiu znacznie szerszemu gronu, niż zakładamy. Zdjęcie z wakacji, lista znajomych czy oznaczenie miejsca zamieszkania mogą być dostępne również dla uczniów, rodziców oraz zupełnie nieznanych osób.

W przypadku nauczyciela szczególnie przydatne jest wyznaczenie granicy między życiem prywatnym a zawodowym. Pomagają w tym odpowiednie ustawienia odbiorców, kontrolowanie oznaczeń oraz regularny przegląd opublikowanych materiałów.

## Jakie informacje warto chronić?

Przeglądając swój profil, zwróć uwagę przede wszystkim na:

- prywatny numer telefonu i adres e-mail;
- pełną datę urodzenia;
- adres zamieszkania oraz zdjęcia pozwalające rozpoznać dom;
- informacje o dzieciach, partnerze i innych członkach rodziny;
- miejsca regularnych spotkań, treningów i wypoczynku;
- informacje o wyjazdach oraz nieobecności w domu;
- zdjęcia dokumentów, biletów, identyfikatorów i korespondencji;
- listę znajomych oraz oznaczenia innych osób.

Pojedynczy wpis może wydawać się nieistotny, lecz kilka publikacji połączonych ze sobą może jednak ujawnić codzienne zwyczaje, relacje rodzinne i miejsca, w których można nas spotkać.

**Przykład:** nauczyciel publikuje zdjęcie sprzed domu, oznacza pobliski klub sportowy i regularnie informuje o godzinach treningów. Osoba przeglądająca profil może na tej podstawie spróbować ustalić okolicę zamieszkania i tygodniowy plan aktywności.

Przed publikacją warto zadać sobie pytanie: **czy chcę, aby tę informację mogła zobaczyć przypadkowa osoba, która zna moje imię i nazwisko?**

## Sprawdzenie obecnej widoczności profilu

Zacznij od ustalenia, co jest już dostępne publicznie.

- Wpisz w wyszukiwarce swoje imię i nazwisko w cudzysłowie, np. „Anna Kowalska”.
- Powtórz wyszukiwanie, dodając miejscowość lub nazwę szkoły.
- Sprawdź wyniki dotyczące profili społecznościowych i zdjęć.
- Otwórz własny profil w oknie prywatnym przeglądarki, bez logowania do serwisu.
- Zapisz, które informacje chcesz ukryć lub usunąć.

Niektóre serwisy wymagają zalogowania, aby wyświetlić profil. Ekran logowania nie potwierdza, że konto jest prywatne. Dlatego później sprawdź również widoczność z perspektywy zalogowanej osoby, która nie należy do Twoich znajomych ani zatwierdzonych obserwujących.

## Facebook - ograniczenie widoczności prywatnego profilu

Ustawienia warto sprawdzić za pomocą narzędzia **Kontrola prywatności**. Prowadzi ono przez kolejne ekrany, na których można zmienić widoczność danych profilowych i publikacji oraz ograniczyć sposoby odnajdywania konta.

Krok 1. Otwórz panel „Kontrola prywatności”

- Otwórz aplikację Facebook i przejdź do **Menu**.
- Wybierz **Ustawienia i prywatność**, a następnie **Ustawienia**.
- Odszukaj i otwórz **Kontrolę prywatności**.
- Pojawi się panel z kolorowymi kafelkami dotyczącymi różnych ustawień konta.




W pierwszej kolejności skorzystaj z dwóch kafelków:

- pomarańczowego — **„Kto może zobaczyć…”**, dotyczącego widoczności udostępnianych informacji;
- fioletowego — **„Jak użytkownicy mogą wyszukać…”**, dotyczącego odnajdywania profilu i nawiązywania kontaktu.

Krok 2. Sprawdź widoczność danych profilowych

Wybierz **pomarańczowy kafelek „Kto może zobaczyć…”** i rozpocznij przegląd. Na ekranie z informacjami profilowymi sprawdź odbiorców poszczególnych danych.

Dla prywatnego profilu zalecane są następujące ustawienia:

| **Informacja** | **Zalecana widoczność** |
|---|---|
| Numer telefonu | Tylko ja |
| Adres e-mail | Tylko ja |
| Dzień i miesiąc urodzenia | Tylko ja lub świadomie wybrane grono znajomych |
| Rok urodzenia | Tylko ja |
| Status związku i informacje rodzinne | Tylko ja lub wybrane osoby |
| Kto może zobaczyć listę Twoich znajomych | Tylko ja |
| Kto może zobaczyć osoby i strony, które obserwujesz | Tylko ja |

Krok 3. Ogranicz odbiorców postów i relacji

Kliknij dalej by przejść do sekcji odbiorców, jest to sekcja gdzie decydujesz kto może zobaczyć Twoje posty i relacje.

Dla prywatnego profilu zalecane są następujące ustawienia:

| **Informacja** | **Zalecana widoczność** |
|---|---|
| Kto może zobaczyć Twoje przyszłe posty i rolki | Znajomi |
| Kto może zobaczyć Twoje relacje | Znajomi |

Następnie skorzystaj z funkcji **ograniczenia widoczności wcześniejszych postów**. Przeczytaj komunikat wyświetlony przez Facebooka i zatwierdź zmianę, jeśli stare publikacje publiczne lub dostępne dla znajomych znajomych chcesz udostępniać węższemu gronu.

Przejdź do kolejnej sekcji klikając przycisk dalej, jest to sekcja dotycząca oznaczania w postach. Zaleca się ustawić w tej sekcji wszystko według zamieszczonego poniżej schematu.




Ustawienie **Znajomi** obejmuje osoby znajdujące się na Twojej liście znajomych. Warto więc przejrzeć również samą listę i ocenić, komu chcesz udostępniać prywatne treści.

**Ważne:** zmiana odbiorców przyszłych postów nie zmienia automatycznie wcześniejszych publikacji. Po zastosowaniu ograniczenia zbiorczego przejrzyj dodatkowo stare zdjęcia i wpisy, szczególnie te zawierające dane rodzinne lub informacje o miejscu zamieszkania.

Krok 4. Ogranicz odnajdywanie profilu i zaproszenia

Wróć do głównego panelu **Kontrola prywatności** i wybierz **fioletowy kafelek „Jak użytkownicy mogą wyszukać…”**. Przejdź przez wyświetlane ustawienia dotyczące odnajdywania konta i kontaktowania się z Tobą.

Zwróć uwagę na:

- **Zaproszenia do znajomych** - jeśli chcesz ograniczyć zaproszenia od przypadkowych osób, wybierz **Znajomi znajomych**.
- **Proponowanie profilu na podstawie numeru telefonu lub adresu e-mail** -wybierz najwęższe dostępne grono, jeśli nie potrzebujesz tej funkcji.
- **Linkowanie do profilu przez wyszukiwarki spoza Facebooka** - wyłącz tę możliwość, jeśli nie chcesz ułatwiać odnajdywania profilu w ten sposób. Nie usuwa to natychmiast wcześniejszych wyników wyszukiwania, ten proces może trochę potrwać.

## Instagram - konto prywatne i kontrola obserwujących

Krok 1. Włącz konto prywatne

- Otwórz swój profil w aplikacji Instagram.

- Dotknij menu z trzema poziomymi liniami.
- W ustawieniach odszukaj Prywatność konta.
- Włącz Konto prywatne i potwierdź zmianę.

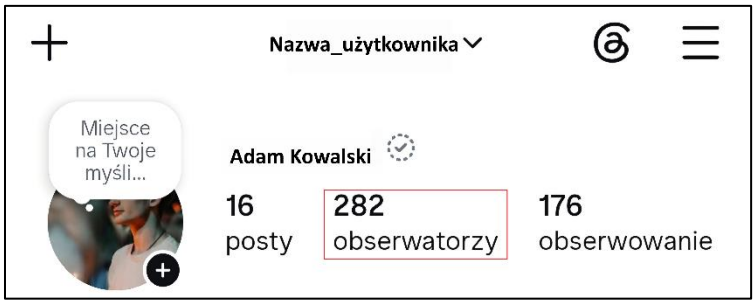
Konto prywatne pozwala ograniczyć dostęp do publikacji i zatwierdzać nowych obserwujących. Jeśli korzystasz z konta firmowego, przed ustawieniem go jako prywatne konieczna jest zmiana na konto osobiste.




Krok 2. Przejrzyj obecnych obserwujących

Samo włączenie prywatności nie zastępuje przeglądu osób, które już obserwują konto.

- Otwórz listę **Obserwujących**.



- Sprawdź, czy rozpoznajesz znajdujące się na niej konta.
- Usuń osoby, którym nie chcesz udostępniać prywatnych publikacji.




- Kolejne prośby o obserwowanie zatwierdzaj świadomie.

Instagram udostępnia też funkcję usuwania obserwujących z konta prywatnego.

Krok 3. Ogranicz oznaczenia i wzmianki

Instagram pozwala osobno ustawić, kto może Cię **oznaczać** oraz kto może dodawać o Tobie **wzmianki**. Obie funkcje tworzą odnośnik do Twojego konta, ale działają inaczej.

| Funkcja | Na czym polega? | Przykład |
|---|---|---|
| Oznaczenie | Autor przypisuje Twoje konto do zdjęcia lub filmu za pomocą funkcji oznaczania osób. Publikacja może pojawić się w zakładce oznaczonych materiałów na Twoim profilu. | Znajomy publikuje wspólne zdjęcie i korzysta z opcji „Oznacz osoby”, wskazując Twoje konto. |
| Wzmianka | Ktoś przywołuje Twoje konto przez wpisanie @nazwy_użytkownika, np. w opisie publikacji, komentarzu lub relacji. Sama wzmianka nie dodaje materiału do zakładki oznaczonych publikacji na Twoim profilu. | Ktoś pisze w komentarzu: „Dziękujemy za spotkanie, @anna_nauczycielka”. |

Oznaczenia dotyczą więc przypisania konta do publikacji, a wzmianki służą przywołaniu konta w treści. Instagram udostępnia ustawienia ograniczające obie te formy kontaktu.

W ustawieniach odszukaj **Znaczniki i wzmianki**. Ogranicz możliwość oznaczania Cię przez przypadkowe konta i włącz ręczne zatwierdzanie oznaczonych publikacji przed ich dodaniem do Twojego profilu.

**Uwaga na określenie „obserwowane osoby".** Chodzi o konta, które **Ty obserwujesz**, a nie o osoby obserwujące Ciebie. Wybierając tę opcję, pozwalasz oznaczać Cię lub dodawać o Tobie wzmianki użytkownikom z Twojej listy **Obserwowani**. Dlatego przejrzyj również tę listę i oceń, komu chcesz pozostawić takie uprawnienia.

- **1. Znaczniki — oznaczanie na zdjęciach i w rolkach**

| Ustawienie | Zalecany wybór |
|---|---|
| Kto może Cię oznaczyć | Zezwalaj na znaczniki od obserwowanych osób |
| Zatwierdzaj znaczniki ręcznie | Włączone |

Ręczne zatwierdzanie pozwala zdecydować, które oznaczone publikacje pojawią się na Twoim profilu. Nie wstrzymuje publikacji materiału u jego autora.

- **2. Wzmianki — przywoływanie konta przez @nazwę_użytkownika**

| Ustawienie | Zalecany wybór |
|---|---|
| Kto może dodawać @wzmianki o Tobie | Zezwalaj na wzmianki tylko od obserwowanych osób |
| Zezwalaj innym na promowanie relacji, w których o Tobie wspomnieli | Wyłączone |
| Zezwalaj innym osobom na promowanie relacji, w których udostępniono Twoje materiały i wspomniano o Tobie | Wyłączone |

## TikTok - ograniczenie dostępu do filmów

Poniższe zalecenia dotyczą osobistego konta nauczyciela. Ustawienia ograniczają dostęp do prywatnych publikacji i ułatwiają kontrolowanie kontaktu z innymi użytkownikami. Nazwy niektórych opcji mogą różnić się między wersjami aplikacji.

Krok 1. Włącz konto prywatne

- Otwórz aplikację TikTok.
- Wybierz **Profil** w dolnej części ekranu.
- Dotknij **Menu** ☰ w prawym górnym rogu.
- Przejdź do **Ustawienia i prywatność à Konto prywatne**
- Włącz **Konto prywatne**.

Przy koncie prywatnym zatwierdzasz osoby, które chcą Cię obserwować i uzyskać dostęp do Twoich publikacji. Nadal można jednak wyszukać konto, a nazwa wyświetlana, nazwa użytkownika i zdjęcie profilowe pozostają publiczne.

Krok 2. Ogranicz proponowanie Twojego konta innym osobom

Przejdź do **Ustawienia i prywatność → Kontakty i lokalizacja**.

Na tym ekranie znajdują się osobne ustawienia dotyczące proponowania Twojego profilu innym osobom, synchronizacji danych oraz lokalizacji.

**Zalecane ustawienia dla prywatnego konta nauczyciela:**

| Sekcja | Ustawienie | Zalecany wybór |
|---|---|---|
| Zasugeruj swoje konto innym | Kontakty | **Wyłączone** |
| Zasugeruj swoje konto innym | Znajomi z Facebooka | **Wyłączone** |
| Zsynchronizuj kontakty i znajomych z Facebooka | Synchronizuj kontakty | **Wyłączone** |
| Zsynchronizuj kontakty i znajomych z Facebooka | Zsynchronizuj znajomych z Facebooka | **Wyłączone** |
| Usługi lokalizacyjne | Dostęp do lokalizacji | **Nigdy** |

**Usuń wcześniej zsynchronizowane dane**

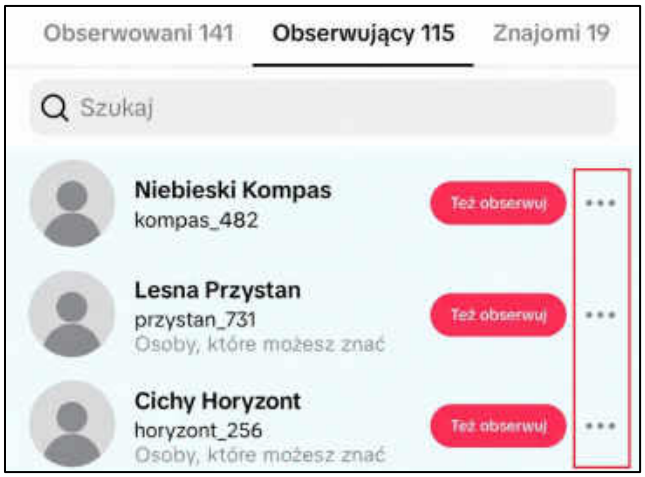
Samo wyłączenie synchronizacji nie usuwa kontaktów przesłanych wcześniej do TikToka. Na ekranie **Kontakty i lokalizacja** sprawdź również opcje:

- **Usuń wcześniej zsynchronizowane kontakty** — wybierz ją, jeżeli jest dostępna, i potwierdź usunięcie.
- **Usuń zsynchronizowanych znajomych z Facebooka** — skorzystaj z niej, jeśli wcześniej synchronizowano listę znajomych.

Jeżeli dana opcja jest wyszarzona i nie można jej wybrać, pomiń ten krok. Nie włączaj synchronizacji tylko po to, aby uaktywnić przycisk usuwania.

Następnie otwórz listę obserwujących. Przejrzyj ją i usuń osoby, którym nie chcesz udostępniać prywatnych materiałów. Funkcję usunięcia obserwującego znajdziesz w menu działań przy danej osobie.




**Uwaga:** konta biznesowe są publiczne. Jeśli korzystasz z takiego konta, ustawienie prywatności wymaga wcześniejszej zmiany jego rodzaju na osobiste.

**Sprawdź również udostępnianie linków**

Wróć do **Ustawień i prywatności**. W sekcji **Interakcje** odszukaj **Wyświetl profil podczas udostępniania linków** i pozostaw tę opcję **wyłączoną**, jeśli nie chcesz pokazywać swojego profilu w związku z udostępnianiem linków.

## Nawyki pomagające oddzielić życie prywatne od pracy

Ustawienia prywatności działają najlepiej w połączeniu ze świadomym publikowaniem.

**Ustal kanał kontaktu ze szkołą.** Do spraw uczniowskich i kontaktu z rodzicami korzystaj z narzędzi przyjętych przez placówkę, np. dziennika elektronicznego lub służbowej poczty. Pozwala to ograniczyć potrzebę udostępniania prywatnego profilu.

**Sprawdzaj tło zdjęć.** Przed publikacją obejrzyj fotografię w powiększeniu. Zwróć uwagę na widoczne dokumenty, nazwiska uczniów, oceny, ekrany komputerów, adresy i identyfikatory.

**Ostrożnie informuj o lokalizacji.** Zdjęcia z wyjazdu możesz opublikować po powrocie. Nie musisz podawać dokładnego miejsca pobytu ani godzin, w których regularnie przebywasz poza domem.

**Ustal zasady z bliskimi.** Poproś rodzinę i znajomych, aby uzgadniali z Tobą publikowanie zdjęć, oznaczanie lokalizacji i udostępnianie informacji o Twoich dzieciach.

**Przeglądaj odbiorców.** Dawny znajomy lub zaakceptowane kiedyś konto nadal może mieć dostęp do nowych publikacji. Co kilka miesięcy oceń, czy obecna lista odbiorców odpowiada Twoim potrzebom.

**Uwzględniaj możliwość wykonania kopii.** Osoba mająca dostęp do publikacji może zrobić zrzut ekranu lub przekazać jej treść dalej. Szczególnie osobiste informacje najlepiej udostępniać bezpośrednio wybranym osobom.

# Rozdział 2. Weryfikacja wycieków danych

## Na czym polegają wycieki danych?

Wyciek danych to sytuacja, w której poufne informacje zostają ujawnione, skopiowane, przekazane lub udostępnione osobom nieupoważnionym do ich posiadania. Wbrew powszechnej opinii, wyciek to nie zawsze spektakularna kradzież z udziałem zaawansowanych hakerów – bardzo często to wynik naszych codziennych, nieświadomych działań. W środowisku szkolnym może to dotyczyć zarówno danych logowania nauczyciela, jak i wrażliwych informacji o uczniach (oceny, opinie z poradni, numery PESEL, adresy zamieszkania) czy rodzicach.

## Do wycieku poufnych informacji może dojść z kilku głównych powodów:

**W wyniku celowego działania, takiego jak na przykład atak cyberprzestępców.** Są to zaplanowane akcje wymierzone w konkretną osobę lub instytucję np. szkołę. Przestępcy wykorzystują do tego celu różne metody:

- **Phishing:** Wysyłanie fałszywych wiadomości e-mail np. podszywających się pod kuratorium, dyrekcję lub administratora dziennika elektronicznego w celu wyłudzenia haseł.
- **Złośliwe oprogramowanie:** Infekowanie szkolnych komputerów wirusami, które kradną zapisane w przeglądarce hasła lub blokują dostęp do plików, żądając okupu.
- **Ataki na infrastrukturę zewnętrzną:** Włamania do baz danych zewnętrznych usługodawców, z których korzysta szkoła np. platformy edukacyjne, sklepy internetowe, w których robimy prywatne zakupy używając tych samych haseł.

**Na skutek przypadkowego błędu, w tym z powodu niewłaściwej konfiguracji systemu.** Błędy technologiczne często wynikają z pośpiechu lub braku odpowiedniej wiedzy przy wdrażaniu narzędzi cyfrowych. Przykłady:

- Udostępnienie folderu na dysku chmurowym (np. Google Drive, OneDrive) z opcją „każdy, kto ma link, może przeglądać” zamiast ograniczenia dostępu tylko dla wybranych osób.
- Pozostawienie szkolnej sieci Wi-Fi bez odpowiedniego zabezpieczenia np. brak hasła, co pozwala osobom z zewnątrz na przechwytywanie przesyłanych danych.
- Błędy w konfiguracji systemów szkolnych, pozwalające uczniom lub rodzicom na wgląd w dokumenty, do których nie powinni mieć dostępu.

**Bezpośrednio w wyniku błędu ludzkiego.** To statystycznie najczęstsza przyczyna wycieków danych na świecie, wynikająca ze zmęczenia, roztargnienia lub niewiedzy. Należą do niej:

- **Pomyłki w adresowaniu e-maili:** Wysłanie tabeli z ocenami lub opinią o uczniu do niewłaściwego rodzica np. o podobnym nazwisku.

- **Brak ukrycia adresatów:** Wysyłanie masowych wiadomości do wszystkich rodziców z użyciem pola „Do” (To) lub „DW” (CC) zamiast „UDW” (BCC), co natychmiast ujawnia wszystkim adresy e-mail pozostałych osób (jest to złamanie przepisów RODO).
- **Zgubienie nośników danych:** Pozostawienie niezabezpieczonego hasłem pendrive'a ze sprawdzianami lub danymi uczniów w sali lekcyjnej, pociągu czy autobusie.
- **Fizyczny dostęp do sprzętu:** Zostawienie włączonego, niezablokowanego komputera na biurku z otwartym dziennikiem elektronicznym podczas przerwy, co daje osobom postronnym swobodny dostęp do danych.

Wśród informacji, które zazwyczaj wyciekają do sieci i wpadają w niepowołane ręce, najczęściej spotyka się:

- Loginy i hasła.
- Adresy e-mail.
- Dane osobowe klientów i kontrahentów, na przykład numery PESEL.
- Poufną korespondencję, dokumenty firmowe oraz różnego rodzaju umowy.

## Dlaczego to takie ważne w pracy nauczyciela?

Nauczyciele na co dzień operują nie tylko własnymi danymi, ale również danymi wrażliwymi uczniów i rodziców, korzystając z dzienników elektronicznych, platform edukacyjnych i dysków chmurowych. Wyciek hasła do prywatnej skrzynki e-mail, jeśli było ono takie samo jak do dziennika elektronicznego, może doprowadzić do poważnego naruszenia bezpieczeństwa całej placówki oświatowej. Dlatego regularna weryfikacja wycieków powinna stać się cyfrowym nawykiem każdego pedagoga.

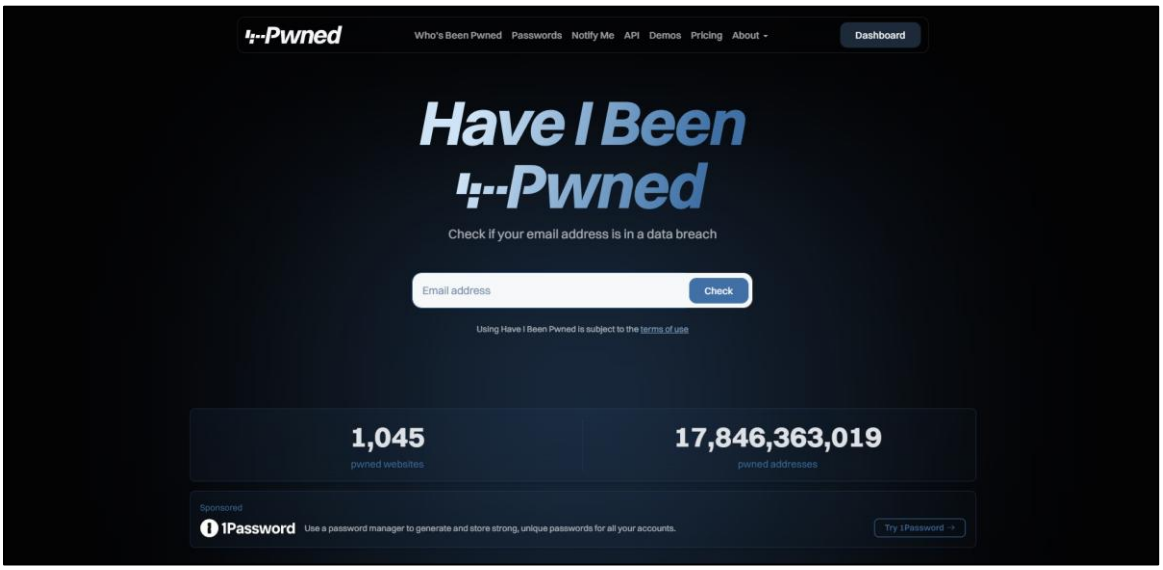
## Jak weryfikować, czy nasze dane wyciekły?

Aby upewnić się, czy nasze służbowe lub prywatne dane nie znalazły się w bazach cyberprzestępców, możemy skorzystać z dedykowanych serwisów. Narzędzia te możemy podzielić na dwie kategorie.

Narzędzia globalne:

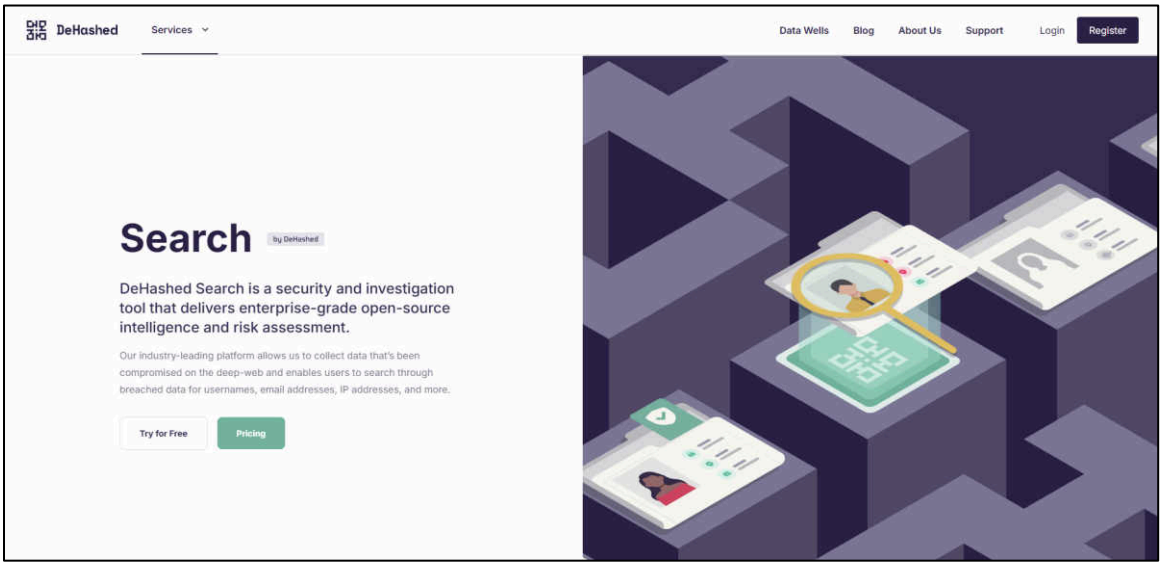
- **Have I Been Pwned** – Jest to darmowa usługa pozwalająca sprawdzić, czy dany adres e-mail lub domena znalazła się w znanych wyciekach danych.

  Link: https://haveibeenpwned.com/.



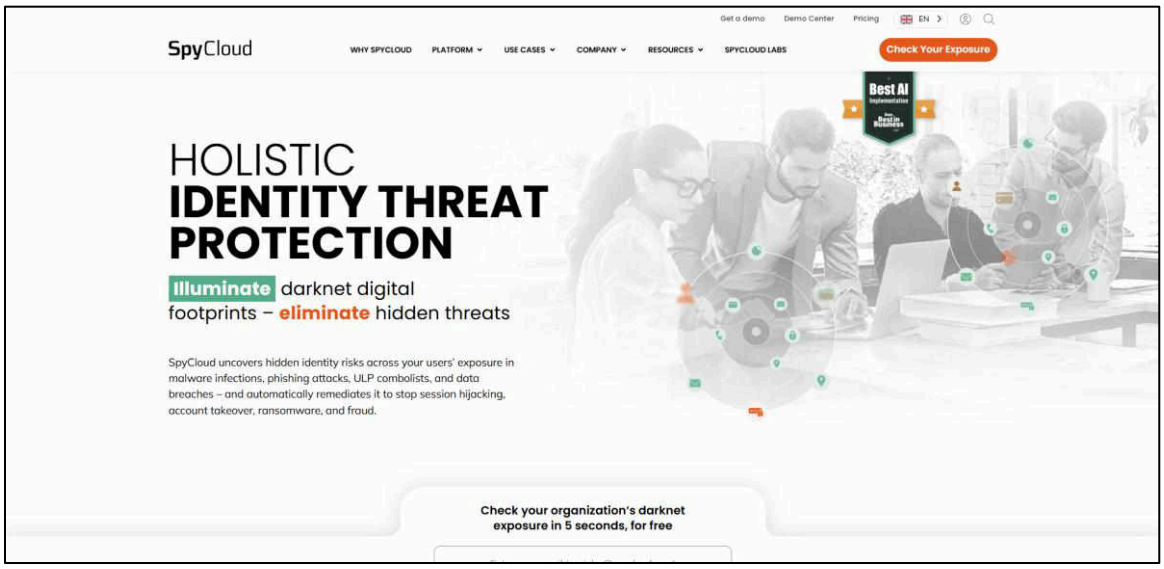

- **DeHashed** – Jest to zaawansowane oraz komercyjne narzędzie OSINT do przeszukiwania baz wycieków. Narzędzie to pozwala na weryfikację nie tylko e-maili, ale też loginów, haseł, adresów IP, numerów telefonów czy nawet nazw użytkownika.

  Link: https://www.dehashed.com/search#breachCheck.




- **SpyCloud** – Jest to zaawansowane narzędzie służące do wykrywania zagrożeń w postaci wycieków w dark webie. Rozwiązanie to umożliwia identyfikację wycieków danych uwierzytelniających i innych informacji wrażliwych. Platforma jest bardzo ceniona za wysoką dokładność detekcji.

  Link: https://spycloud.com.

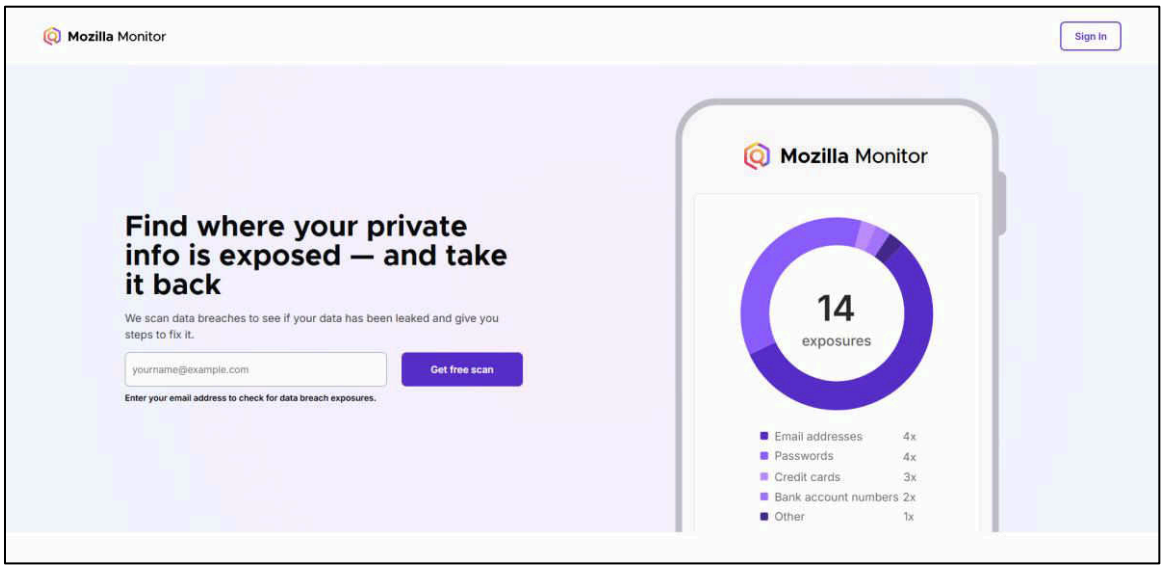



Dodatkowe darmowe narzędzia wspierające:

- **Bezpiecznedane.gov.pl** – Oficjalny polski serwis rządowy, który pozwala sprawdzić, czy nasze dane logowania znalazły się w bazach udostępnionych przez cyberprzestępców. Logowanie odbywa się bezpiecznie za pomocą Profilu Zaufanego lub aplikacji mObywatel.




- **Firefox Monitor (monitor.firefox.com)** – Usługa, która działa w oparciu o popularne bazy wycieków, ale dodatkowo pozwala na skonfigurowanie darmowych alertów. Po założeniu konta system automatycznie wyśle powiadomienie na Twój adres e-mail, jeśli w przyszłości pojawi się on w jakimkolwiek nowym wycieku.




## Co zrobić, gdy odkryjemy, że nasze dane wyciekły?

Samo potwierdzenie wycieku to dopiero pierwszy krok. Najważniejsza jest natychmiastowa i właściwa reakcja. Jeśli jedno z narzędzi wykaże, że Twoje dane zostały skompromitowane, podejmij następujące działania:

1. **Zmień hasło natychmiast:** Zaloguj się do serwisu, z którego nastąpił wyciek, i natychmiast zmień hasło na nowe, silne i unikalne.
2. **Zastosuj zasadę "braku recyklingu haseł":** Jeśli używałeś tego samego hasła na innych stronach (np. w dzienniku elektronicznym, poczcie służbowej, systemach bankowych), musisz bezwzględnie zmienić je również tam. Przestępcy często automatycznie sprawdzają wyciekłe hasła w innych portalach.
3. **Włącz uwierzytelnianie dwuetapowe (2FA):** Jeśli usługa na to pozwala, natychmiast włącz logowanie dwuskładnikowe wymagające np. dodatkowego kodu z SMS lub aplikacji Authenticator. Dzięki temu, nawet jeśli przestępca zdobędzie Twoje hasło, nie zaloguje się bez dostępu do Twojego telefonu.
4. **Zastrzeż numer PESEL:** Jeżeli w wycieku znalazły się Twoje dane wrażliwe (jak numer PESEL), niezwłocznie zastrzeż go za pomocą aplikacji mObywatel lub na stronie obywatel.gov.pl. Uchroni Cię to m.in. przed wzięciem przez oszustów pożyczki na Twoje nazwisko.
5. **Zachowaj wzmożoną czujność:** Po wycieku danych szczególnie adresu e-mail i numeru telefonu spodziewaj się zwiększonej liczby podejrzanych SMS-ów, fałszywych linków czy telefonów od oszustów podszywających się pod pracowników banku lub kurierów.

# Rozdzial 3. Jak nie dać się złapać na phishing

Phishing to metoda oszustwa, w której przestępca podszywa się pod zaufaną instytucję (np. Ministerstwo Edukacji Narodowej, dostawcę e-dziennika, dyrekcję lub rodzica), aby wyłudzić dane logowania, informacje o uczniach lub zainfekować komputer.

## Jakie najczęściej nauczyciel może dostawać maile od cyberprzestępców?

- **Fałszywy e-dziennik:** E-maile z informacją o "konieczności aktualizacji konta" lub "nowej wiadomości od dyrekcji" z linkiem prowadzącym do strony łudząco podobnej do prawdziwego panelu logowania.
- **Wiadomości od „rodzica”:** Maile zawierające zainfekowane załączniki, których nazwy mają wywołać niepokój lub pilną reakcję, np. skarga_na_nauczyciela.zip, zwolnienie_lekarskie_jan_kowalski.docx lub wniosek_do_dyrekcji.pdf.exe.
- **Komunikaty od "administracji IT" lub "kuratorium":** Pilne wezwania do zmiany hasła pod groźbą zablokowania dostępu do szkolnej poczty lub platformy Microsoft Teams
- **Ataki na komunikatorach:** Zhakowane konta innych nauczycieli rozsyłające przez E-dziennik lub Teams prośby o drobną pożyczkę (tzw. oszustwo na BLIK) lub linki do "ciekawych materiałów na lekcję".

## Jak rozpoznać próbę oszustwa?

- **Presja czasu i negatywne emocje:** Zachowaj ostrożność wobec wiadomości wymuszających natychmiastowe działanie, np. „Twoje konto zostanie zablokowane za 24 godziny!” lub „Ostatnie ostrzeżenie!”. Oszuści wywołują strach, niepokój albo ciekawość, aby skłonić odbiorcę do kliknięcia linku, otwarcia załącznika lub podania danych bez zastanowienia.
- **Podejrzany adres nadawcy:** Nie sugeruj się samą nazwą wyświetlaną, np. „Dyrektor szkoły” czy „Administracja dziennika”. Kliknij lub rozwiń pole „Od”, aby sprawdzić pełny adres e-mail. Zwróć uwagę na literówki, dodatkowe znaki oraz adresy inne niż te, których dana osoba lub instytucja zwykle używa. Pamiętaj, że nawet wiadomość z prawidłowego adresu może pochodzić z przejętego konta.
- **Adres ukryty pod linkiem:** Napis „Zaloguj się do dziennika” nie potwierdza, dokąd prowadzi odnośnik. Na komputerze najedź kursorem na link bez klikania i odczytaj adres wyświetlany w dolnej części okna lub w podpowiedzi. Na telefonie przytrzymaj odnośnik i sprawdź jego adres w wyświetlonym menu. Szukaj literówek i nazw jedynie przypominających właściwą witrynę. Jeśli masz wątpliwości, otwórz usługę ze swojej zapisanej zakładki.
- **Nietypowy język i sposób powitania:** Sygnałem ostrzegawczym mogą być błędy językowe, dziwny szyk zdań, nietypowy dla nadawcy ton oraz ogólne powitania, np. „Drogi Użytkowniku”. Nie traktuj jednak poprawnej polszczyzny, profesjonalnego wyglądu ani użycia Twojego imienia jako dowodu autentyczności. Oszuści również potrafią przygotować przekonującą, poprawnie napisaną wiadomość.

- **Zwracaj uwagę na domenę**, czyli nazwę witryny w adresie. Poniższe adresy służą wyłącznie jako przykłady.

| **Przykładowy adres** | **Co z niego wynika** |
|---|---|
| https://dziennik.example.org/logowanie | Dziennik jest subdomeną example.org. |
| https://example.org.pomoc.example.net/logowanie | Nazwa example.org jest częścią dłuższej nazwy. W tym przykładzie domeną jest example.net. |
| https://example.net/example.org/logowanie | Adres prowadzi do example.net. Napis example.org znajduje się jedynie w ścieżce. |

**HTTPS oznacza szyfrowanie połączenia, a nie potwierdzenie uczciwości strony.** Fałszywa witryna również może korzystać z HTTPS.

## Zasady bezpieczeństwa

- **Weryfikowanie innym kanałem:** Dziwne prośby od dyrektora, nauczycieli oraz pracowników szkoły zweryfikuj innym kanałem – zadzwoń, napisz SMS lub zapytaj osobiście
- **Nie otwieraj podejrzanych załączników:** Szczególna ostrożność przy plikach .zip, .rar, .exe oraz dokumentach pakietu Office, które po otwarciu proszą o "włączenie makr" lub "włączenie edycji".
- **Wpisuj adresy ręcznie:** Zamiast klikać w link z e-maila "Zaloguj się, aby odczytać wiadomość", otwórz nową kartę i wejdź na stronę dziennika ze swojej zapisanej zakładki.
- **Ograniczone zaufanie w pokoju nauczycielskim:** Zawsze blokuj ekran komputera (Windows + L) i wylogowuj się ze szkolnych platform na współdzielonych urządzeniach. Oszustwo może przyjść z konta kolegi/koleżanki, która zapomniała się wylogować.

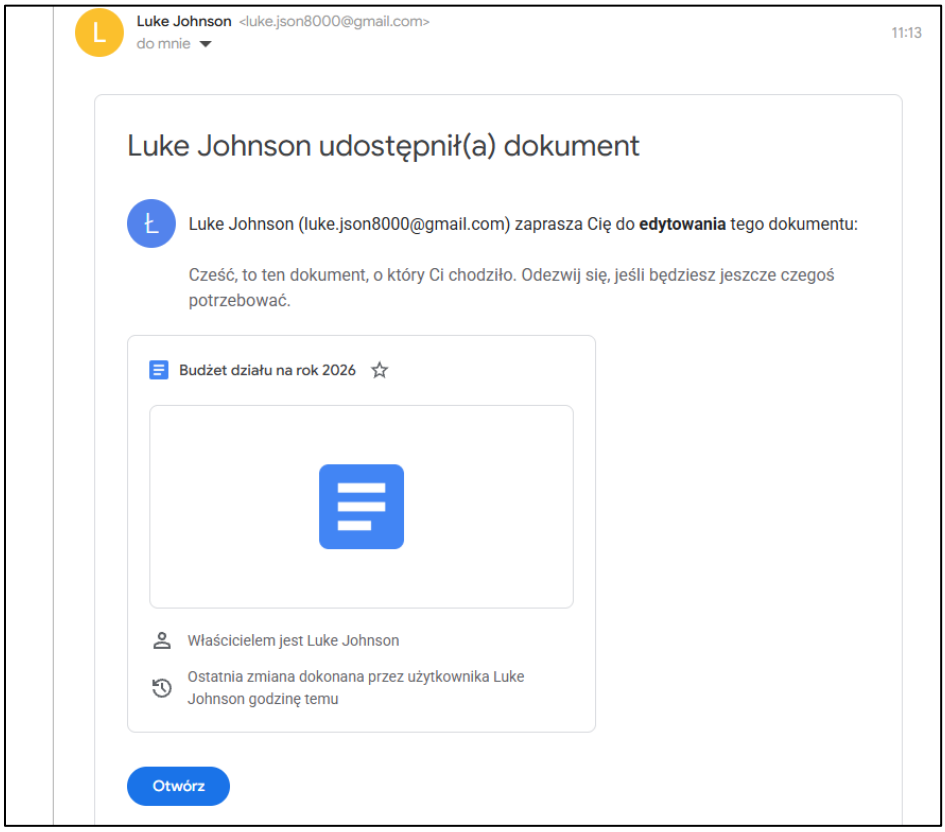
## Co zrobić w przypadku kliknięcia w złośliwy link?

- **Nie panikuj, ale działaj szybko:** Natychmiast zmień hasło do skompromitowanego serwisu (z innego, bezpiecznego urządzenia).
- **Zgłoś incydent:** Poinformuj szkolnego administratora IT lub inspektora ochrony danych (IOD). Jeśli wyciekło hasło do dziennika, mogą być zagrożone dane wrażliwe uczniów.
- **Wyloguj wszystkie sesje:** W ustawieniach konta (np. Google lub Microsoft) skorzystaj z opcji wylogowania ze wszystkich aktywnych urządzeń.

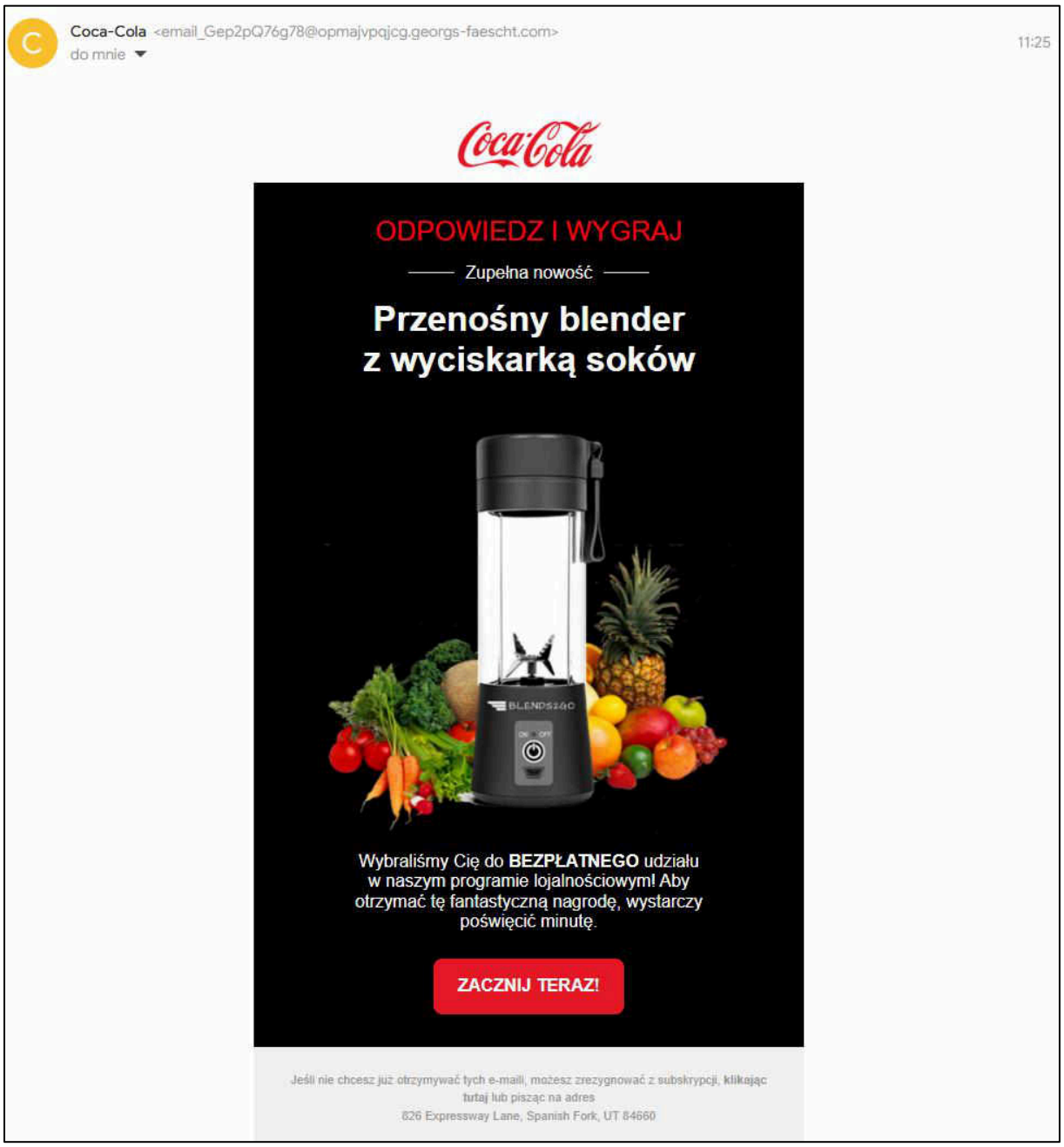
## Pułapki przy nieznanych linkach

- **Fałszywa strona logowania (Kradzież tożsamości):**
  Link przenosi Cię na stronę, która wygląda *identycznie* jak logowanie do poczty szkolnej, e-dziennika lub banku. Gdy odruchowo wpiszesz login i hasło, trafiają one prosto do bazy danych hakera. Od tego momentu przestępca ma dostęp do Twoich wiadomości i danych uczniów.
- **Automatyczne pobranie złośliwego kodu (Drive-by download):**
  Samo wejście na zainfekowaną stronę może wykorzystać lukę w Twojej przeglądarce (jeśli np. nie jest zaktualizowana). Złośliwy program (np. wirus szpiegujący lub oprogramowanie szyfrujące dysk – ransomware) pobiera się i instaluje w tle, bez pytania o zgodę.
- **Kradzież sesji (Ciasteczek):**
  Jeśli jesteś już zalogowany w innej karcie do e-dziennika lub Facebooka, złośliwy link może zawierać skrypt (wykorzystujący lukę w zabezpieczeniach np. przeglądarki), który wykradnie Twoją "aktywną sesję". Haker uzyska dostęp do Twojego konta bez konieczności znania hasła.
- **Potwierdzenie, że "jesteś na celowniku":**
  Każdy link phishingowy ma często przypisany unikalny kod dla Twojego adresu e-mail. Jeśli klikniesz, system oszustów odnotowuje: *"Ten adres e-mail jest aktywny, a właściciel klika w linki"*. Od tego momentu zaczniesz otrzymywać znacznie więcej spamu i bardziej wyrafinowanych ataków.

Przykłady phisingu:



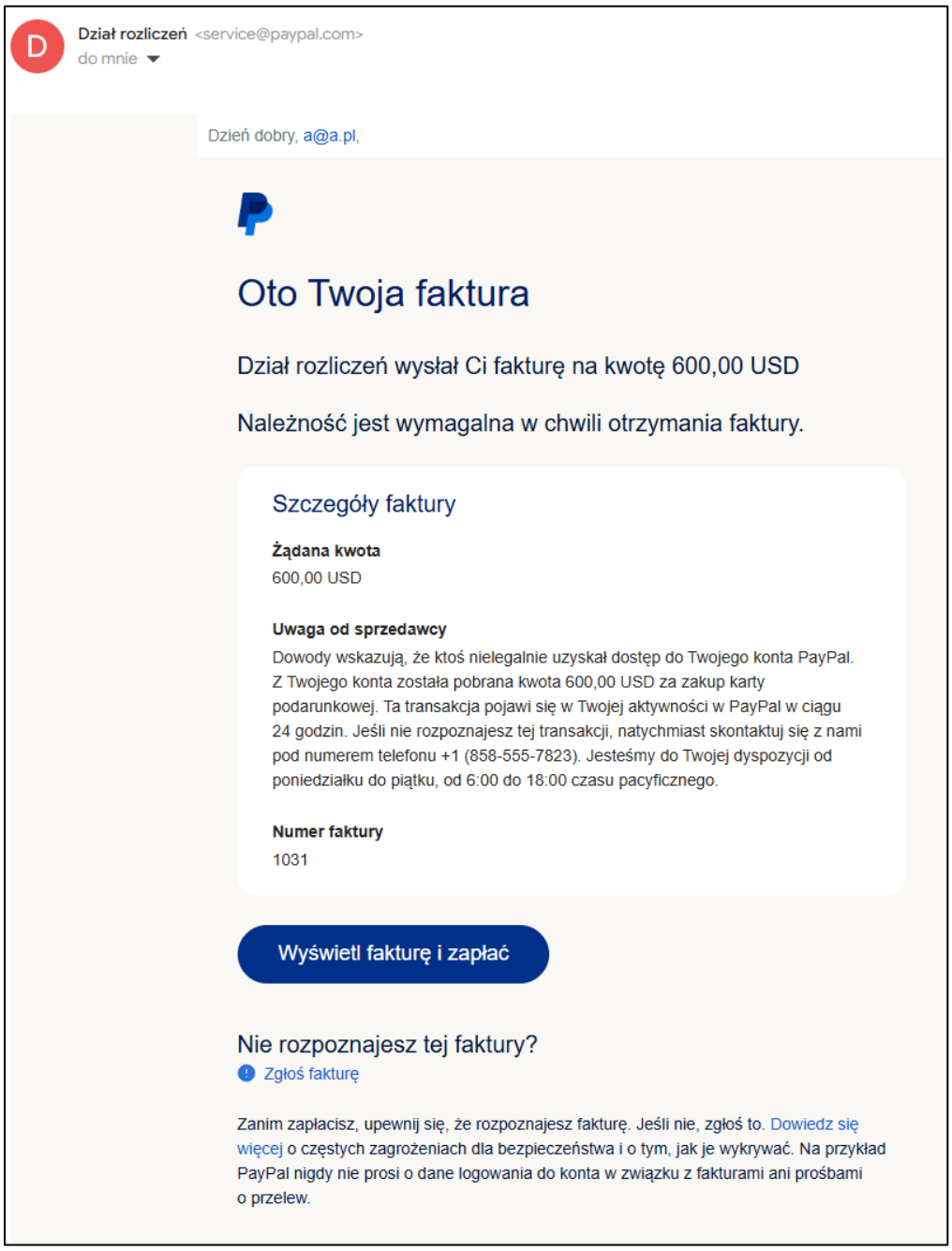

Najechanie na ten link wskaźnikiem myszy lub jego przytrzymanie powoduje wyświetlenie informacji o tym, że prowadzi on do niezabezpieczonej domeny „drive --google.com", która naśladuje inną.




E-mail wydaje się pochodzić od Coca-Coli, ale adres nadawcy jest bardzo przypadkowy. Nie oznacza to, że e-mail jest nieprawdziwy, ale jest to sygnał ostrzegawczy. Treść, w tym tekst, znajduje się na obrazie.

Chociaż ta technika jest używana w niektórych prawidłowych wiadomościach, służy też do unikania wykrycia.

Adres URL ma za zadanie ukryć przekierowania, ale jednocześnie uniknąć wykrycia przez dostawcę usług hostingowych, uruchamiając tylko tekst po znaku „#” (zwykle jest to krótki kod używany do linkowania do określonej lokalizacji na stronie).



D

**Dział rozliczeń** <service@paypal.com>
do mnie

Dzień dobry, a@a.pl,

## Oto Twoja faktura

Dział rozliczeń wysłał Ci fakturę na kwotę 600,00 USD

Należność jest wymagalna w chwili otrzymania faktury.

### Szczegóły faktury

**Żądana kwota**
600,00 USD

**Uwaga od sprzedawcy**
Dowody wskazują, że ktoś nielegalnie uzyskał dostęp do Twojego konta PayPal. Z Twojego konta została pobrana kwota 600,00 USD za zakup karty podarunkowej. Ta transakcja pojawi się w Twojej aktywności w PayPal w ciągu 24 godzin. Jeśli nie rozpoznajesz tej transakcji, natychmiast skontaktuj się z nami pod numerem telefonu +1 (858-555-7823). Jesteśmy do Twojej dyspozycji od poniedziałku do piątku, od 6:00 do 18:00 czasu pacyficznego.

**Numer faktury**
1031

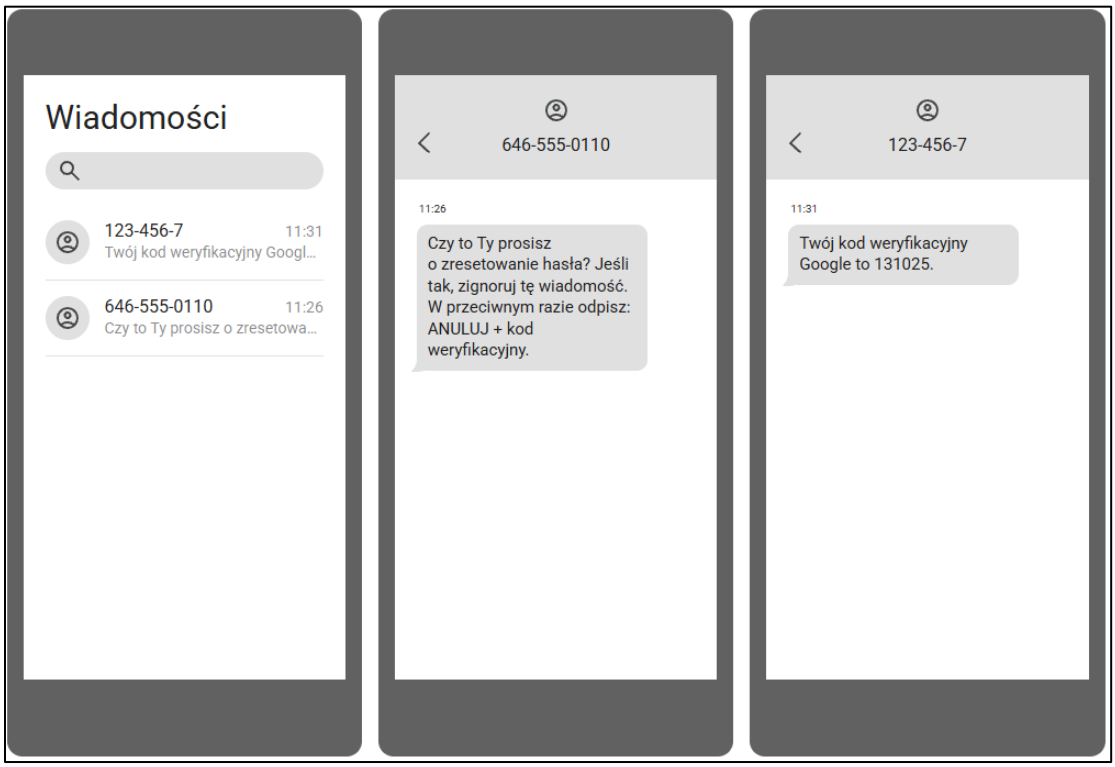
Wyświetl fakturę i zapłać

Nie rozpoznajesz tej faktury?
Zgłoś fakturę

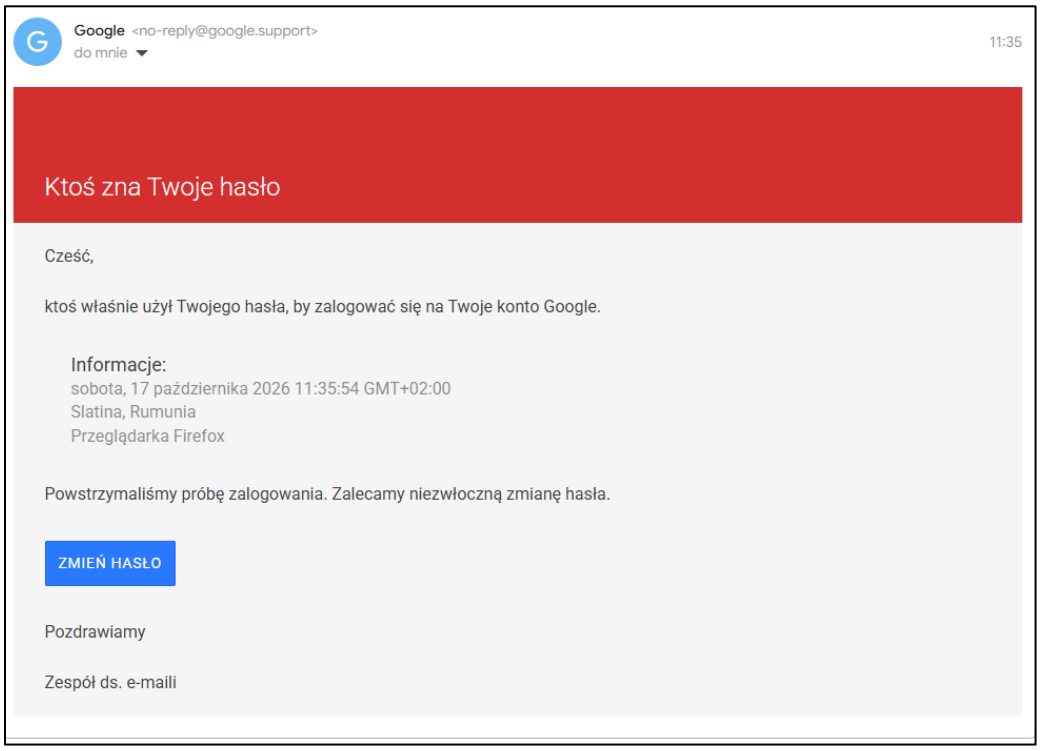
Zanim zapłacisz, upewnij się, że rozpoznajesz fakturę. Jeśli nie, zgłoś to. Dowiedz się więcej o częstych zagrożeniach dla bezpieczeństwa i o tym, jak je wykrywać. Na przykład PayPal nigdy nie prosi o dane logowania do konta w związku z fakturami ani prośbami o przelew.

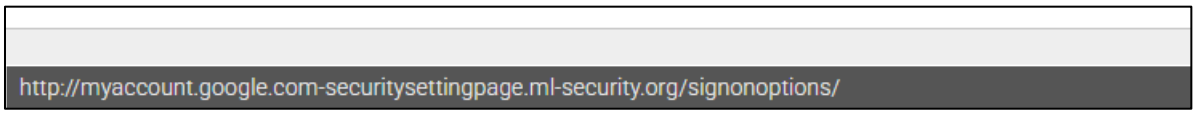
Ta wiadomość to tak naprawdę „Uwaga od sprzedawcy". Oszuści wywołali poczucie pilności, co jest częstym sposobem na skłonienie użytkowników do podjęcia określonych działań.

Przestępcy mają nadzieję, że zadzwonisz pod ten numer, a oni będą mogli kontynuować oszustwo. Numery telefonów wiarygodnych firm możesz zweryfikować na ich stronach internetowych (np. w witrynie PayPal).



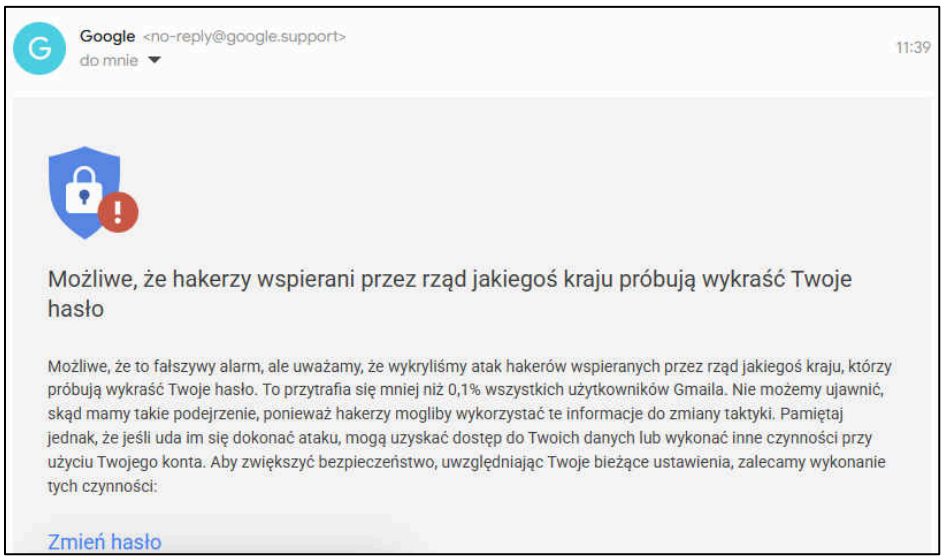

Nigdy nie przekazuj innym osobom kodów logowania, kodów weryfikacji dwuetapowej ani kodów autoryzujących transakcje — również podczas rozmowy z osobą podającą się za pracownika banku. Kod wpisuj wyłącznie w oficjalnej aplikacji lub na sprawdzonej stronie usługi, podczas czynności, którą sam rozpocząłeś. Przed zatwierdzeniem operacji przeczytaj jej opis i sprawdź, czy szczegóły się zgadzają. Jeśli usługa na to pozwala, korzystaj z odpornych na phishing metod logowania, takich jak klucze dostępu lub klucze bezpieczeństwa FIDO2.

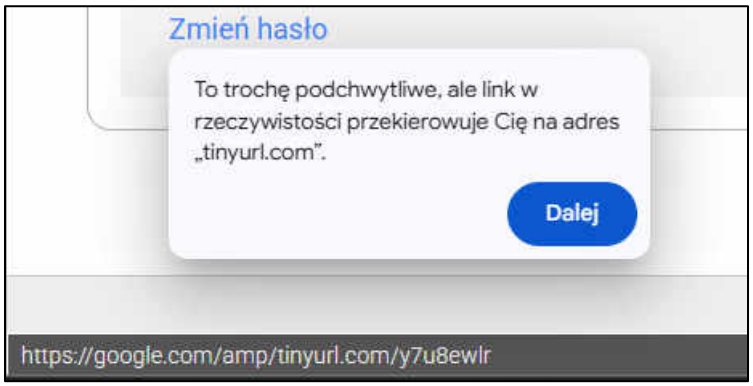





Adres nadawcy „google.support” nie jest używany.

Link prowadzi do subdomeny „ml-security.org”, a nie domeny google.



# Rozdział 4. Tworzenie haseł, zarządzanie hasłami i weryfikacja dwuetapowa

## Dlaczego tradycyjne podejście do haseł już nie wystarcza?

Hasło to pierwsza, a w wielu przypadkach wciąż jedyna bariera chroniąca **poufność** i **integralność** informacji w systemach. Za pojedynczym ciągiem znaków kryje się dostęp do służbowej skrzynki pocztowej, arkuszy z danymi poufnymi, opinii z poradni psychologiczno-pedagogicznych oraz danych osobowych setek osób. W terminologii cyberbezpieczeństwa słabe lub powtarzalne hasło stanowi krytyczną **podatność** (lukę w zabezpieczeniach), której wykorzystanie przez osoby nieuprawnione prowadzi bezpośrednio do **incydentu bezpieczeństwa** oraz naruszenia przepisów RODO.

Przez lata wokół tworzenia haseł narosło wiele szkodliwych mitów. Wymuszanie haseł składających się z trudnych do zapamiętania kombinacji znaków (np. K#9$mP!2x) sprawiło, że użytkownicy zaczęli zapisywać je na żółtych karteczkach przyklejanych do monitora lub stosować przewidywalne schematy typu **Wrzesien2026!**. Dla współczesnych programów łamiących zabezpieczenia odgadnięcie takiego schematu zajmuje ułamki sekund.

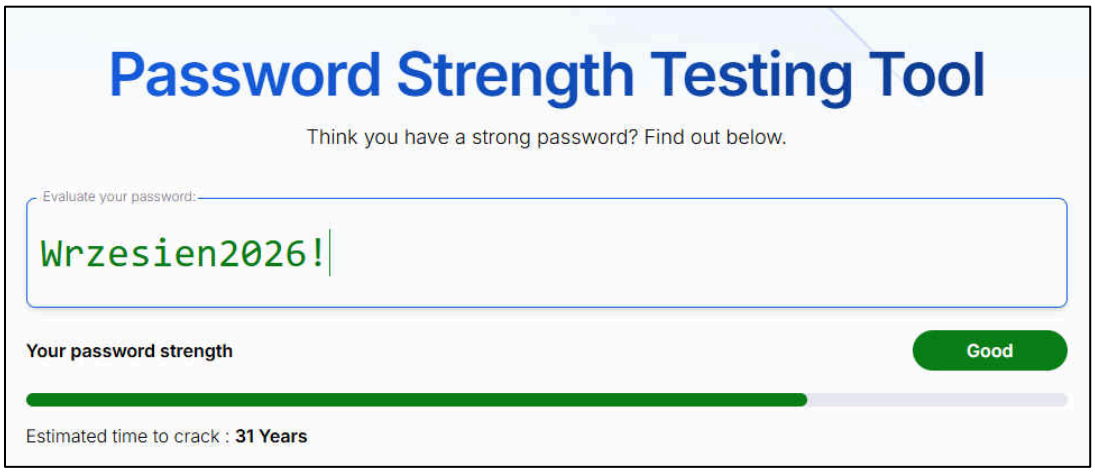
## Jak tworzyć pancerne hasła, które łatwo zapamiętać?

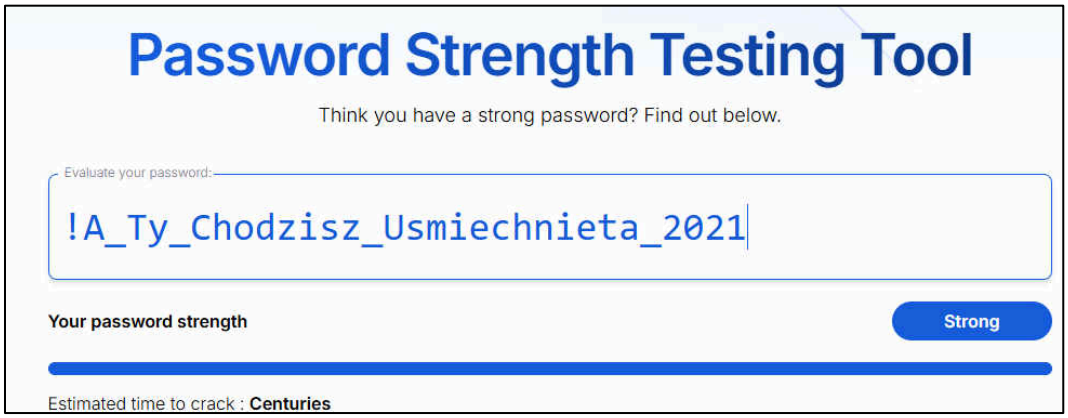
Współczesne standardy bezpieczeństwa odchodzą od krótkich, skomplikowanych ciągów znaków na rzecz tzw. **haseł-zdań**. Matematyka stojąca za łamaniem haseł jest bezwzględna: dla algorytmów przestępców znacznie większą przeszkodą jest **długość hasła** niż tylko jego pozorna zawiłość.

Podczas tworzenia silnego hasła należy kierować się następującymi zasadami:

- **Długość ma kluczowe znaczenie:** Bezpieczne hasło powinno składać się z minimum **14 znaków**, a w przypadku kluczowych kont nawet z kilkunastu lub ponad dwudziestu znaków.
- **Stosowanie metody fraz (haseł-zdań):** Zamiast pojedynczego słowa warto utworzyć absurdalne, łatwe do wyobrażenia zdanie złożone z 4–5 niepowiązanych ze sobą słów, przedzielonych znakami specjalnymi lub cyframi, np. **Niebieski-Slon-Spiewa-W-Klasie-44!** Takie hasło ma aż 35 znaków, jest niemal niemożliwe do złamania metodą siłową, a jednocześnie zapada w pamięć znacznie łatwiej niż losowy ciąg ośmiu znaków.

- **Unikanie słów słownikowych i danych łatwych do odgadnięcia:** W hasłach nie należy wykorzystywać imion członków rodziny, nazw zwierząt domowych, dat urodzenia. Informacje te można w kilka minut pozyskać z mediów społecznościowych lub strony internetowej placówki.
- **Odrzucenie prostych zamienników:** Zamiana litery „a” na „@”, „o” na „0” czy „s” na „$” (np. N@uczyciel2026!) jest doskonale znana programom hakerskim i jest sprawdzana w pierwszej kolejności.




## Efekt domina – dlaczego każde konto musi mieć inne hasło?

Jednym z najpoważniejszych błędów w higienie cyfrowej jest **recykling haseł**, czyli używanie tego samego hasła w wielu różnych miejscach. W praktyce często wygląda to tak, że jedno wybrane hasło otwiera prywatną skrzynkę pocztową, konto w małym sklepie internetowym z pomocami dydaktycznymi, forum dla nauczycieli oraz szkolny dziennik elektroniczny.

Cyberprzestępcy nie muszą włamywać się bezpośrednio do pilnie strzeżonego systemu e-dziennika. Wystarczy, że wykradną bazę danych ze słabo zabezpieczonego sklepu internetowego lub portalu hobbystycznego, w którym osoba założyła konto kilka lat wcześniej. Następnie specjalne boty automatycznie próbują dopasować wykradzioną parę „adres e-mail + hasło" do setek innych popularnych serwisów: poczty elektronicznej, platformy Microsoft Teams, dysków chmurowych czy innych systemów. Jeśli hasło było wszędzie takie samo, włamanie do jednego, mało istotnego serwisu powoduje efekt domina i utratę kontroli nad wszystkimi kontami służbowymi oraz prywatnymi.

**Złota zasada bezpieczeństwa:** Do każdego serwisu należy stosować zupełnie inne, unikalne hasło, a przynajmniej do każdego ważnego serwisu.

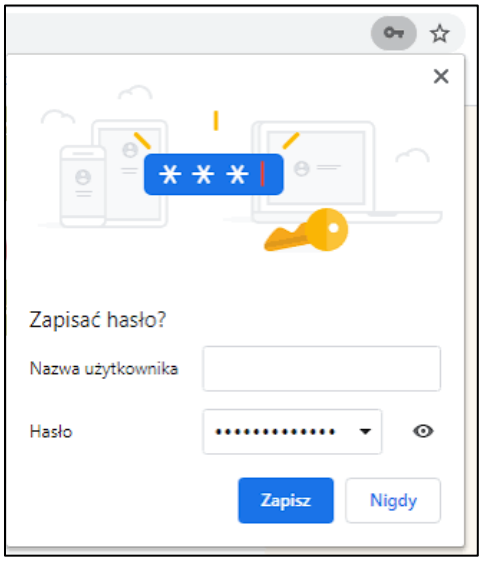
## Menedżery haseł – osobisty cyfrowy sejf

Zapamiętanie kilkudziesięciu długich i unikalnych haseł przekracza możliwości ludzkiej pamięci. Rozwiązaniem tego problemu nie jest jednak zapisywanie ich w zeszycie ani w pliku tekstowym hasla.txt na pulpicie komputera, lecz wykorzystanie **menedżera haseł**.

Menedżer haseł to specjalny, zaszyfrowany program pełniący funkcję cyfrowego sejfu. Użytkownik musi pamiętać wyłącznie **jedno silne hasło główne**, które otwiera dostęp do sejfu. Wszystkie pozostałe hasła są przez program automatycznie generowane jako długie, losowe ciągi znaków, bezpiecznie przechowywane i automatycznie uzupełniane na odpowiednich stronach internetowych. Co więcej, menedżer haseł stanowi doskonałą ochronę przed phishingiem – nie wpisze on hasła na fałszywej stronie podszywającej się pod portal, ponieważ rozpozna, że domena nie zgadza się z oryginałem.

## Dlaczego zapisywanie haseł w przeglądarce na szkolnym komputerze to pułapka?

Podczas logowania przeglądarki internetowe (Chrome, Edge, Firefox) proponują zapamiętanie hasła. **Zaleca się wyłączenie tej funkcji zarówno na komputerach służbowych, jak i prywatnych oraz korzystanie z osobnego menedżera haseł.** Dostęp nieupoważnionej osoby do niezablokowanego urządzenia lub infekcja złośliwym oprogramowaniem mogą zagrozić przechowywanym danym logowania. Wybrany menedżer zabezpiecz silnym hasłem głównym i włącz jego automatyczną blokadę. Pamiętaj również o blokowaniu ekranu za każdym razem, gdy odchodzisz od komputera.



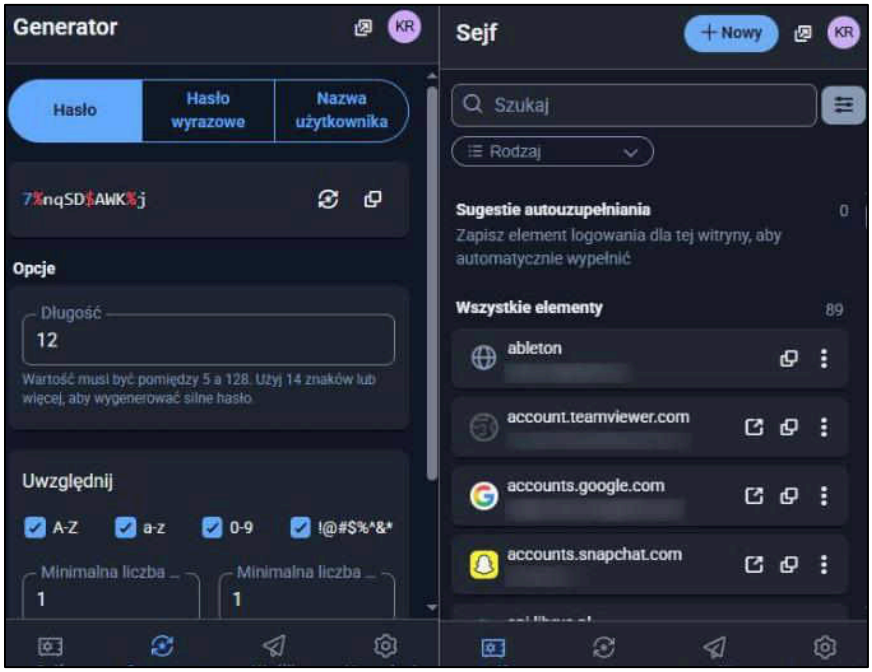

## Sprawdzone i bezpieczny menedżer haseł

W codziennej pracy warto korzystać z dedykowanych, niezależnych menedżerów haseł, które szyfrują dane jeszcze przed wysłaniem ich do chmury lub przechowują je wyłącznie lokalnie:

1. **Bitwarden** – Jeden z najpopularniejszych na świecie menedżerów haseł typu *open-source* (o otwartym kodzie źródłowym, regularnie audytowanym przez niezależnych ekspertów).

W podstawowej wersji jest całkowicie darmowy, działa na komputerach i smartfonach. Posiada wiele zaawansowanych funkcji w czym również wbudowany generator silnych haseł i fraz.

Link: https://bitwarden.com/




2. **KeePassXC** – Darmowy i niezwykle bezpieczny menedżer haseł działający całkowicie offline. Baza haseł zapisywana jest w postaci silnie zaszyfrowanego pliku bezpośrednio na dysku komputera lub na prywatnym pendrive'ie, bez przesyłania jakichkolwiek informacji do chmury.
   Link: https://keepassxc.org

3. **Proton Pass / 1Password** – Zaawansowane narzędzia oferujące wysoki poziom szyfrowania, automatyczne wykrywanie wyciekłych haseł oraz możliwość bezpiecznego współdzielenia wybranych danych logowania.
   Linki:
   - https://proton.me/pass
   - https://1password.com

## Weryfikacja dwuetapowa (2FA / MFA) – tarcza na wypadek kradzieży hasła

Nawet najsilniejsze hasło może zostać wykradzione, jeśli komputer jest zainfekowany złośliwym oprogramowaniem lub użytkownik da się nabrać na przekonywujący atak phishingowy. Dlatego kluczowym elementem ochrony kont jest **weryfikacja dwuetapowa**, określana również jako uwierzytelnianie wieloskładnikowe.

Mechanizm ten opiera się na połączeniu co najmniej dwóch niezależnych czynników:

1. **Czegoś, co się wie** – czyli loginu i hasła.
2. **Czegoś, co się posiada** – np. smartfona z aplikacją generującą jednorazowe kody lub fizycznego klucza bezpieczeństwa.

Weryfikacja dwuetapowa znacznie podnosi poziom bezpieczeństwa, skutecznie blokując próby nieautoryzowanego dostępu. Aby zalogować się na nowym urządzeniu, trzeba dodatkowo podać jednorazowy, 6-cyfrowy kod, który zmienia się co 30 sekund w aplikacji na telefonie właściciela konta, lub zatwierdzić logowanie fizycznym kluczem.

## Jakie metody weryfikacji dwuetapowej są najbezpieczniejsze?

- **Kody SMS (ochrona podstawowa):** Po wpisaniu hasła system wysyła kod SMS na przypisany numer telefonu.
- **Aplikacje uwierzytelniające – Authenticator:** Specjalne aplikacje instalowane na smartfonie, które generują jednorazowe kody czasowe nawet wtedy, gdy telefon nie ma dostępu do internetu ani zasięgu sieci komórkowej. Kody nie są przesyłane przez sieć, dzięki czemu nie można ich przechwycić w drodze do odbiorcy.
- **Klucze dostępu oraz fizyczne klucze bezpieczeństwa U2F/FIDO2:** Rozwiązania całkowicie odporne na phishing. Fizyczny klucz (wyglądający jak mały pendrive, np. YubiKey) podłącza się do portu USB lub przykłada zbliżeniowo (NFC) do telefonu. Klucz weryfikuje prawdziwość domeny – nawet jeśli użytkownik wejdzie na idealnie podrobioną stronę e-dziennika, klucz odmówi autoryzacji logowania.

## Polecane aplikacje do weryfikacji dwuetapowej (2FA)

1. **Google Authenticator** – Prosta i darmowa aplikacja na systemy Android oraz iOS, pozwalająca na szybkie dodawanie kont za pomocą zeskanowania kodu QR wyświetlanego na ekranie komputera.
2. **Microsoft Authenticator** – Niezwykle przydatna w szkołach korzystających z ekosystemu Microsoft 365 oraz platformy Microsoft Teams. Oprócz standardowych kodów umożliwia zatwierdzenie logowania powiadomieniem Push z dopasowaniem wyświetlanej liczby.
   Link: https://www.microsoft.com/pl-pl/security/mobile-authenticator-app
3. **Ente Auth / Aegis Authenticator** – Cenione aplikacje, oferujące dodatkowe zabezpieczenie samej aplikacji odciskiem palca oraz bezpieczne szyfrowane kopie zapasowe kodów na wypadek zgubienia lub uszkodzenia telefonu.
   Link: https://ente.io/auth/

## Polityka bezpieczeństwa haseł w pracy – podsumowanie organizacyjne

Zarządzanie dostępem w placówce oświatowej wymaga nie tylko narzędzi technicznych, ale również przestrzegania wewnętrznych procedur składających się na **politykę bezpieczeństwa informacji**:

- **Kategoryczny zakaz współdzielenia kont:** Niedopuszczalne jest pożyczanie swojego loginu i hasła do e-dziennika innym osobom (np. na czas zastępstwa).

- **Rozdział sfery służbowej od prywatnej:** Służbowy adres e-mail oraz hasła wykorzystywane w szkole nie powinny być używane do rejestracji w prywatnych serwisach zakupowych, społecznościowych czy rozrywkowych.
- **Kiedy zmieniać hasło?** Nowoczesne wytyczne cyberbezpieczeństwa (m.in. NASK oraz NIST) wskazują, że wymuszana zmiana silnego, długiego hasła co 30 dni przynosi odwrotny skutek, skłaniając ludzi do tworzenia haseł słabszych i różniących się tylko jedną cyfrą na końcu. Długie i unikalne hasło chronione przez 2FA należy jednak zmienić **natychmiast** w sytuacji podejrzenia wycieku danych, po wpisaniu go na podejrzanej stronie lub po zalogowaniu się na niezaufanym komputerze.

# Rozdział 5. Kanały komunikacji z uczniami, rodzicami oraz pracownikami.

## Dlaczego komunikatory na social mediach są złe w pracy nauczyciela?

**Ochrona danych i szkolne zasady komunikacji:** Do kontaktu w sprawach uczniowskich korzystaj z narzędzi zatwierdzonych przez szkołę. Nie przesyłaj ocen, informacji o zdrowiu ani dokumentacji uczniów przez prywatne konta i grupy w komunikatorach. Szkoła, przy wsparciu IOD, powinna ocenić podstawę prawną, warunki korzystania z danej usługi oraz zabezpieczenia danych. Samo korzystanie z serwerów zewnętrznego dostawcy nie oznacza automatycznie naruszenia RODO.

**Utrata kontroli nad sytuacjami kryzysowymi:** Jeśli konto ucznia na platformie społecznościowej zostanie przejęte przez hakera i na klasowej grupie zaczną pojawiać się złośliwe linki (phishing) lub nieodpowiednie treści, jesteście bezradni. Jako "admini" grupy na Messengerze nie możecie zresetować hasła ofierze ani trwale zablokować konta oszusta. W systemach szkolnych taki incydent zgłaszacie szkolnemu administratorowi, który jednym kliknięciem odcina zagrożenie.

**Zatarcie granic i wypalenie zawodowe:** Uczeń piszący na prywatny profil o 22:00 narusza Waszą przestrzeń osobistą i prawo do odpoczynku. Cyfrowa dostępność "na wyciągnięcie ręki" sprawia, że praca płynnie rozlewa się na czas wolny. Tworzy to presję natychmiastowej odpowiedzi, co drastycznie przyspiesza wypalenie zawodowe.

**Zagrożenie dla autorytetu:** Obecność w tej samej przestrzeni wirtualnej i posiadanie uczniów lub rodziców w znajomych na prywatnych profilach zaciera profesjonalny dystans. Komunikacja często traci formalny charakter, co utrudnia późniejsze egzekwowanie obowiązków edukacyjnych.

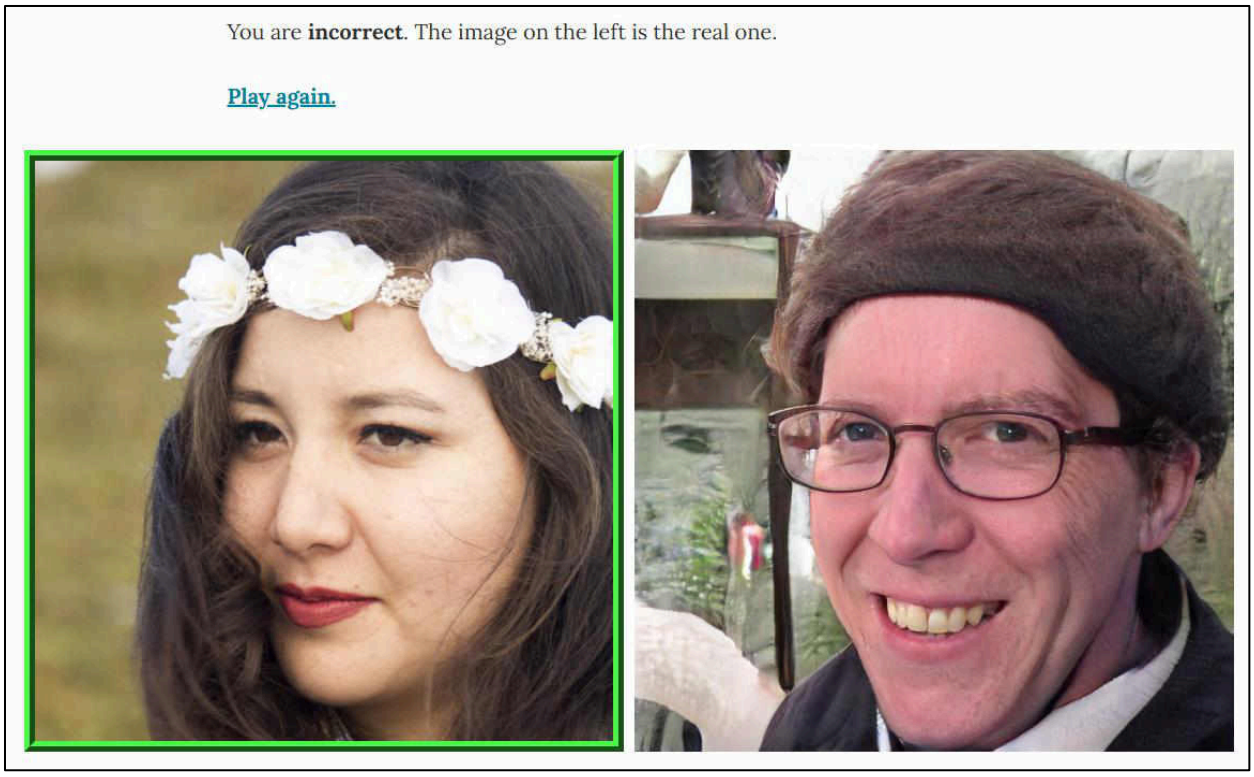
| Narzędzie | Zastosowanie w pracy nauczyciela | Korzyść dla bezpieczeństwa i komfortu |
|---|---|---|
| Librus (E-dziennik) | Formalna komunikacja z rodzicami, komunikaty o sprawdzianach, oceny, wezwania, zwolnienia. | System w 100% zgodny z polskim prawem oświatowym. Wiadomości w Librusie stanowią oficjalną, wiarygodną dokumentację, która bezdyskusyjnie chroni Was w przypadku ewentualnych sporów z rodzicami. |
| Microsoft Teams | Codzienna praca z klasą, przesyłanie materiałów, szybkie pytania edukacyjne od uczniów, oddawanie prac. | Pełna kontrola administracyjna szkoły i wbudowane filtry bezpieczeństwa. Zapewnia wyraźny podział – to uczeń loguje się do "wirtualnej klasy", aby z Wami porozmawiać, a nie Wy wchodzicie do jego komunikatora. |
| Służbowy E-mail | Wymiana obszerniejszych dokumentów, kontakt z dyrekcją, instytucjami zewnętrznymi, dłuższe opinie. | Tworzy w pełni profesjonalny wizerunek. Znacznie ułatwia kategoryzację wiadomości, przeszukiwanie ustaleń i archiwizację korespondencji. |

# Rozdział 6. Deepfake i pułapki w AI

## Czym jest technologia Deepfake i jak zmienia postrzeganie prawdy w sieci?

Rozwój generatywnej sztucznej inteligencji doprowadził do sytuacji, w której powiedzenie „zobaczyć znaczy uwierzyć" całkowicie straciło swoją aktualność. Jednym z najpoważniejszych współczesnych **zagrożeń** dla **integralności** informacji jest technologia **Deepfake**. Polega ona na wykorzystywaniu zaawansowanych algorytmów sztucznej inteligencji do tworzenia lub modyfikowania obrazów, nagrań wideo oraz próbek głosu w taki sposób, że są one niemal nieodróżnialne od autentycznych materiałów.

W dzisiejszych czasach technologia ta przestaje być wyłącznie ciekawostką technologiczną, a staje się realnym narzędziem wykorzystywanym do dezinformacji, oszustw finansowych oraz nowoczesnych form cyberprzemocy. Aby stworzyć fotorealistyczny fotomontaż lub wygenerować nagranie wideo, w którym dana osoba wypowiada słowa, których nigdy nie użyła, współczesnym aplikacjom wystarczy zaledwie jedno zdjęcie pobrane ze strony internetowej lub kilkunastosekundowa próbka głosu zarejestrowana podczas rozmowy.




## Najczęstsze zagrożenia związane z Deepfake w środowisku szkolnym

Wykorzystanie syntetycznych mediów w placówkach oświatowych przybiera kilka szczególnie niebezpiecznych form:

- **Naruszenie wizerunku i cyberprzemoc wobec nauczycieli oraz uczniów:** Za pomocą darmowych aplikacji dostępnych w sieci możliwe jest nałożenie twarzy nauczyciela lub ucznia na dowolny materiał wideo lub wygenerowanie ośmieszających, a niekiedy

wręcz kompromitujących grafik. Takie działania prowadzą do poważnych **incydentów bezpieczeństwa**, godzących w dobra osobiste oraz autorytet pedagoga.

- **Klonowanie głosu i oszustwa telefoniczne:** Przestępcy mogą pobrać krótki fragment wypowiedzi z publicznie dostępnych filmów w mediach społecznościowych szkoły, a następnie wygenerować syntetyczny głos o identycznej barwie i intonacji. Taki głos jest wykorzystywany w atakach socjotechnicznych – np. do wykonania telefonu lub wysłania wiadomości głosowej na komunikatorze z pilną prośbą o pożyczkę kodem BLIK lub przekazanie poufnych danych.
- **Fabrykowanie fałszywych dowodów:** Spreparowane nagrania audio lub zmanipulowane obrazy mogą zostać wykorzystane do bezpodstawnego oskarżenia pracownika szkoły lub ucznia o nieetyczne zachowanie czy użycie słów, które w rzeczywistości nigdy nie padły.

## Jak rozpoznać materiał Deepfake?

Choć algorytmy sztucznej inteligencji stale się doskonalą, podczas uważnej obserwacji zdjęcia lub nagrania wideo często można dostrzec charakterystyczne niedoskonałości:

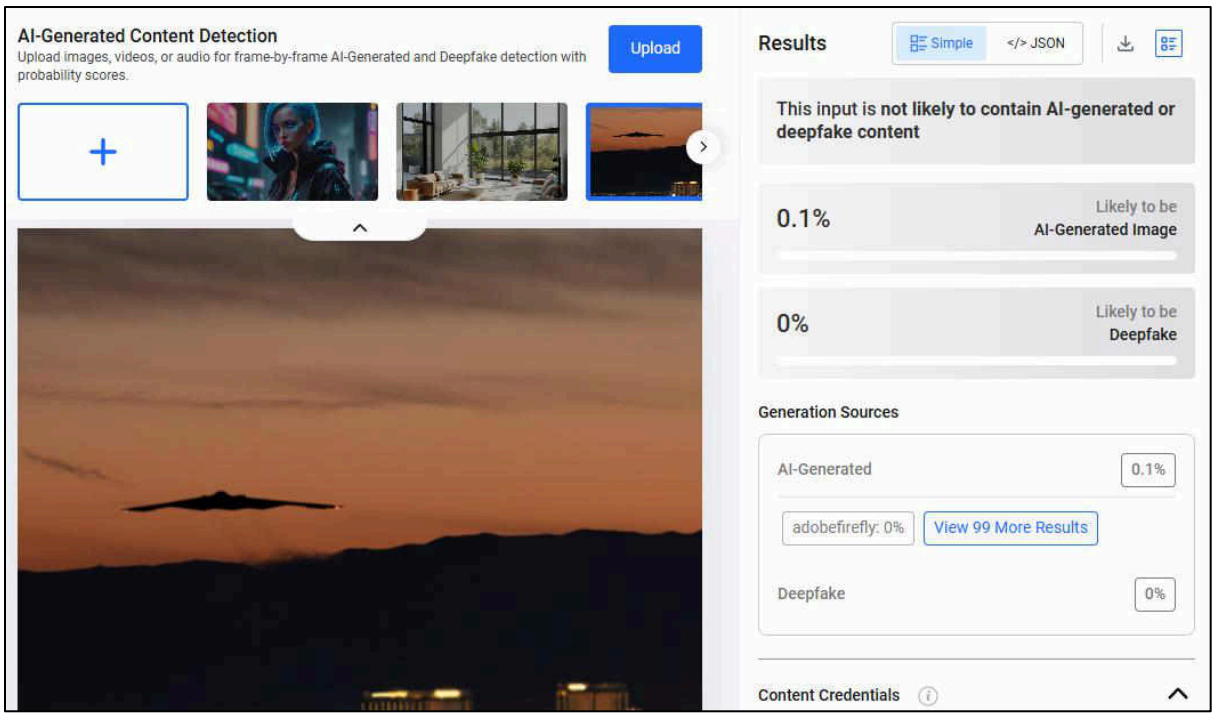
- **Nienaturalna mimika i ruch oczu:** Osoba na nagraniu może mrugać zbyt rzadko, zbyt często lub w sposób mechaniczny. Spojrzenie bywa **„puste”** i **nieskoordynowane** z ruchem głowy.
- **Zniekształcenia na granicach twarzy i w detalach:** Warto zwrócić uwagę na krawędzie żuchwy, linię włosów, uszy oraz oprawki okularów, które przy ruchu głowy mogą się **rozmywać** lub delikatnie **migotać**. Na wygenerowanych zdjęciach błędy często pojawiają się w obrębie dłoni **(zbyt duża lub mała liczba palców, nienaturalne wygięcia)**, zębów oraz napisów w tle (przypominających niezrozumiałe symbole).
- **Brak synchronizacji ruchu warg z dźwiękiem:** W nagraniach wideo ruch ust może minimalnie rozmijać się z wypowiadanymi słowami lub wyglądać na sztucznie doklejony do statycznej twarzy.
- **Anomalie dźwiękowe:** W przypadku sklonowanego głosu można niekiedy wychwycić jednostajny, pozbawiony naturalnych emocji ton, brak oddechów pomiędzy długimi zdaniami lub nietypowe akcentowanie polskich wyrazów.

## Narzędzia do weryfikacji, czy materiał to Deepfake lub wytwór AI

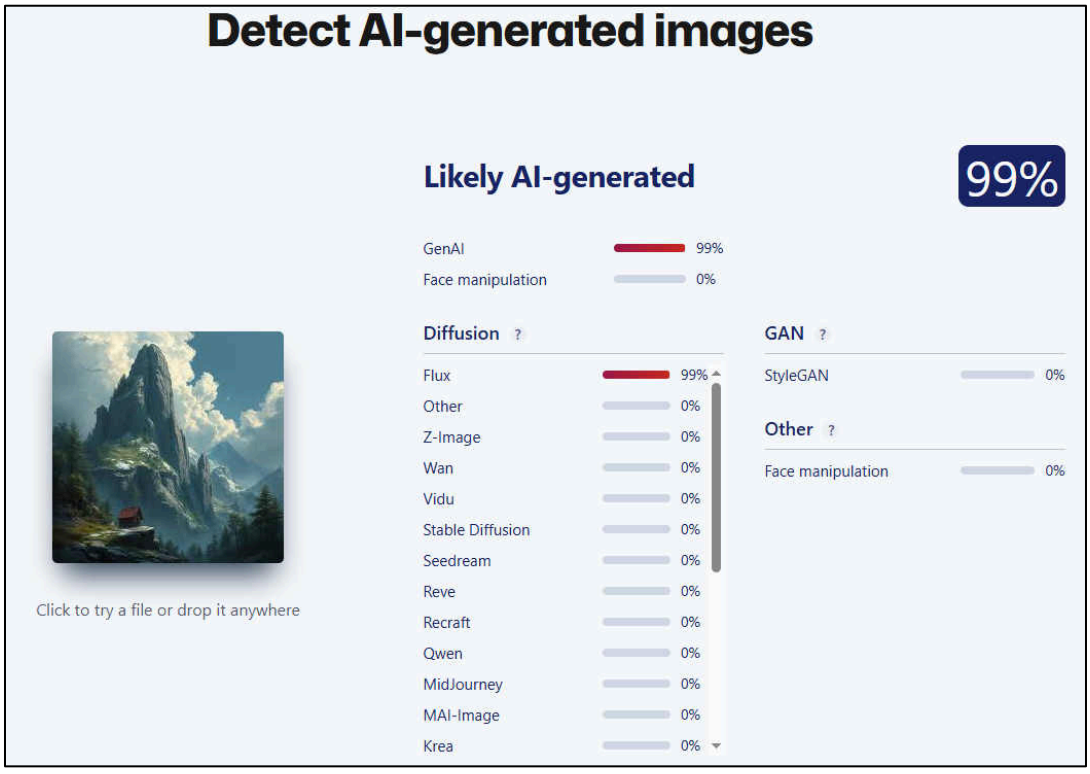
Gdy zachodzi podejrzenie, że zdjęcie, tekst lub nagranie wideo zostało wygenerowane przez sztuczną inteligencję, poza oceną wzrokową warto wykorzystać specjalistyczne narzędzia analityczne:

1. **Hive Moderation** – Jedno z najdokładniejszych narzędzi dostępnych z poziomu przeglądarki internetowej. Pozwala na bezpłatne przesłanie pliku graficznego, nagrania audio, wideo lub fragmentu tekstu. System analizuje materiał i określa procentowe prawdopodobieństwo użycia konkretnych generatorów (np. Midjourney, DALL-E, Stable Diffusion czy ChatGPT).

Link: https://hivemoderation.com/ai-generated-content-detection




2. **Sightengine** – Zaawansowany detektor pozwalający w kilka sekund zweryfikować, czy podejrzane zdjęcie jest autentyczną fotografią, czy obrazem wygenerowanym przez sztuczną inteligencję lub zmodyfikowanym metodą Deepfake.
   Link: https://sightengine.com/detect-ai-generated-images



3. **Obiektyw Google (Google Lens) oraz TinEye https://tineye.com/)** – Narzędzia do tzw. wstecznego wyszukiwania obrazem. Choć nie są typowymi detektorami AI, pozwalają błyskawicznie sprawdzić, czy kontrowersyjne zdjęcie pojawiło się wcześniej w internecie w zupełnie innym kontekście i czy nie zostało przerobione z oryginalnej fotografii.

## Pułapki AI – jakich danych bezwzględnie NIE należy wprowadzać do czatbotów?

Generatywna sztuczna inteligencja (taka jak ChatGPT, Microsoft Copilot, Google Gemini czy Claude) stanowi ogromne wsparcie w pracy dydaktycznej – pomaga tworzyć scenariusze lekcji, quizy, kryteria oceniania czy dopasowywać materiały do potrzeb uczniów. Korzystanie z tych narzędzi wiąże się jednak z poważną pułapką dotyczącą **poufności** informacji.

Domyślnie większość publicznie dostępnych, darmowych czatbotów AI traktuje wpisywane przez użytkowników polecenia oraz załączane pliki jako materiał szkoleniowy **do trenowania kolejnych wersji swoich modeli**. Oznacza to, że każda informacja wpisana w okno czatu trafia na zewnętrzne serwery korporacji technologicznych, może być **przeglądana** przez audytorów jakości, a w skrajnych przypadkach – zostać ujawniona innym użytkownikom na świecie. Wprowadzenie danych chronionych do publicznego modelu AI jest równoznaczne z ich **wyciekiem** oraz naruszeniem przepisów RODO.

## Czarna lista danych – czego nie wolno wpisywać i wgrywać do AI:

- **Danych osobowych uczniów, rodziców i pracowników szkoły:** Imion i nazwisk, numerów PESEL, dat urodzenia, adresów zamieszkania, numerów telefonów oraz adresów e-mail.
- **Dokumentacji psychologiczno-pedagogicznej i medycznej:** Bezwzględnie zabrania się wklejania treści opinii oraz orzeczeń z poradni psychologiczno-pedagogicznych (np. w celu „szybkiego wygenerowania IPET-u" lub streszczenia zaleceń), a także notatek służbowych dotyczących sytuacji rodzinnej, zdrowotnej czy emocjonalnej ucznia.
- **Arkuszy ocen i dokumentacji przebiegu nauczania:** Zestawień ocen przypisanych do konkretnych nazwisk, list obecności, protokołów posiedzeń rady pedagogicznej oraz wewnętrznych pism, umów i regulaminów szkolnych.
- **Wizerunków uczniów i nauczycieli:** Przesyłanie zdjęć z wycieczek czy wydarzeń szkolnych do generatorów AI (np. w celu usunięcia tła, poprawy jakości lub przerobienia zdjęcia klasowego na styl komiksowy) oznacza przekazanie biometrycznych danych wizerunkowych zewnętrznemu podmiotowi bez podstawy prawnej.
- **Danych uwierzytelniających:** Haseł, loginów, kodów dostępu oraz poufnej korespondencji służbowej .

## Pułapka „halucynacji AI" w materiałach edukacyjnych

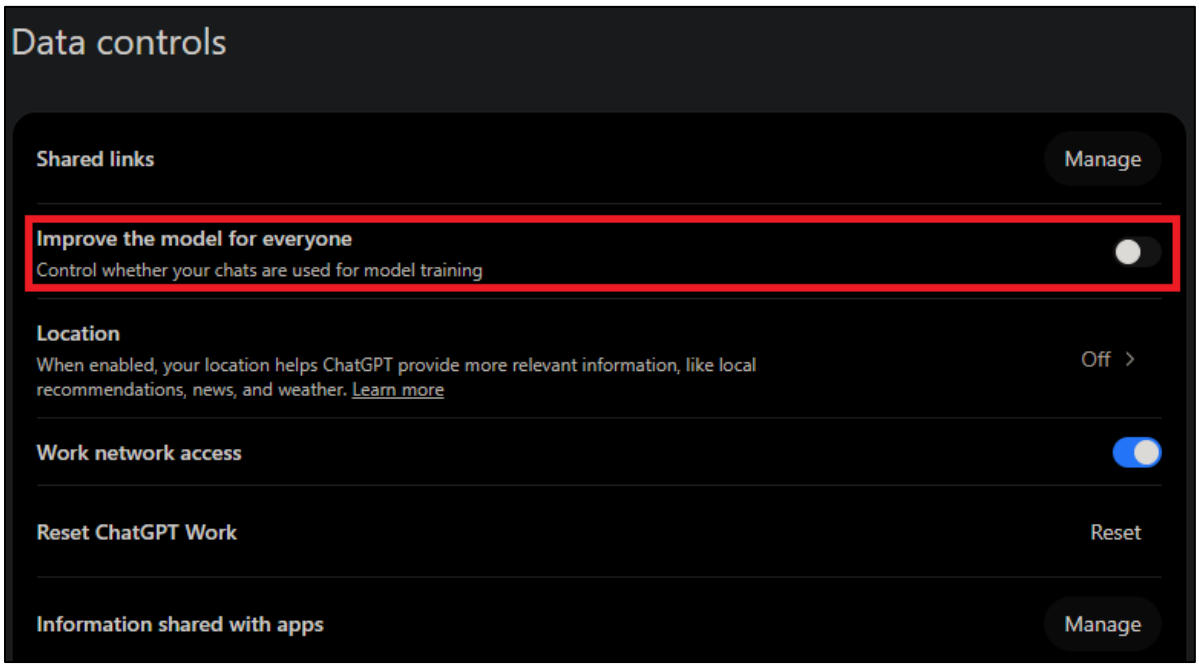
Kolejnym zagrożeniem wynikającym z bezkrytycznego zaufania do sztucznej inteligencji są tzw. **halucynacje**. Modele językowe **nie „wiedzą", co jest prawdą** – ich zadaniem jest przewidywanie najbardziej prawdopodobnego kolejnego słowa w zdaniu. Z tego

powodu czatbot potrafi w niezwykle przekonujący i profesjonalnie brzmiący sposób zmyślić fakty historyczne, podać błędne wzory chemiczne, przytoczyć nieistniejące przepisy prawa oświatowego lub wygenerować bibliografię składającą się z książek, których nikt nigdy nie napisał. Każdy materiał dydaktyczny wygenerowany przy wsparciu AI wymaga bezwzględnej weryfikacji merytorycznej.

## Jak bezpiecznie korzystać ze sztucznej inteligencji?

Aby czerpać korzyści z narzędzi AI bez narażania placówki na **incydent bezpieczeństwa**, w codziennej pracy oraz w ramach szkolnej **polityki bezpieczeństwa** należy stosować trzy podstawowe zasady:

1. **Bezwzględna anonimizacja danych:** Przed poproszeniem czatbota o pomoc w opracowaniu dostosowań edukacyjnych lub zredagowaniu trudnego pisma, należy usunąć z tekstu wszelkie dane pozwalające na identyfikację osób. Zamiast wklejać skan orzeczenia konkretnego ucznia, należy wpisać ogólny komunikat, np.: *„Zaproponuj formy pracy na lekcji matematyki dla ucznia klasy VI z dysleksją i trudnościami w koncentracji uwagi”*.
2. **Wyłączenie trenowania modeli na danych użytkownika:** W ustawieniach najpopularniejszych narzędzi AI można zablokować wykorzystywanie prowadzonych rozmów do szkolenia sztucznej inteligencji. W serwisie ChatGPT należy wejść w Ustawienia -> Kontrola danych i wyłączyć opcję *„Ulepszaj model dla wszystkich”*.




3. **Korzystanie ze szkolnych środowisk zamkniętych:** Jeżeli szkoła posiada wdrożony pakiet Microsoft 365 lub Google Workspace dla Edukacji, zaleca się korzystanie z narzędzi AI wbudowanych w te pakiety, które posiadają umowne gwarancje ochrony danych i nie wykorzystują informacji wprowadzanych przez użytkowników do trenowania publicznych modeli.

# Rozdział 7. Bezpieczeństwo fizycznych urządzeń

W dzisiejszym cyfrowym świecie ochrona naszych danych to nie tylko silne hasła w internecie, ale również odpowiednie zabezpieczenie fizycznych urządzeń, z których korzystamy na co dzień. Telefony i komputery przechowują mnóstwo naszych poufnych informacji. Poniżej przedstawiono zbiór najważniejszych zasad i dobrych praktyk, które pomogą uchronić sprzęt i dane przed niepowołanym dostępem.

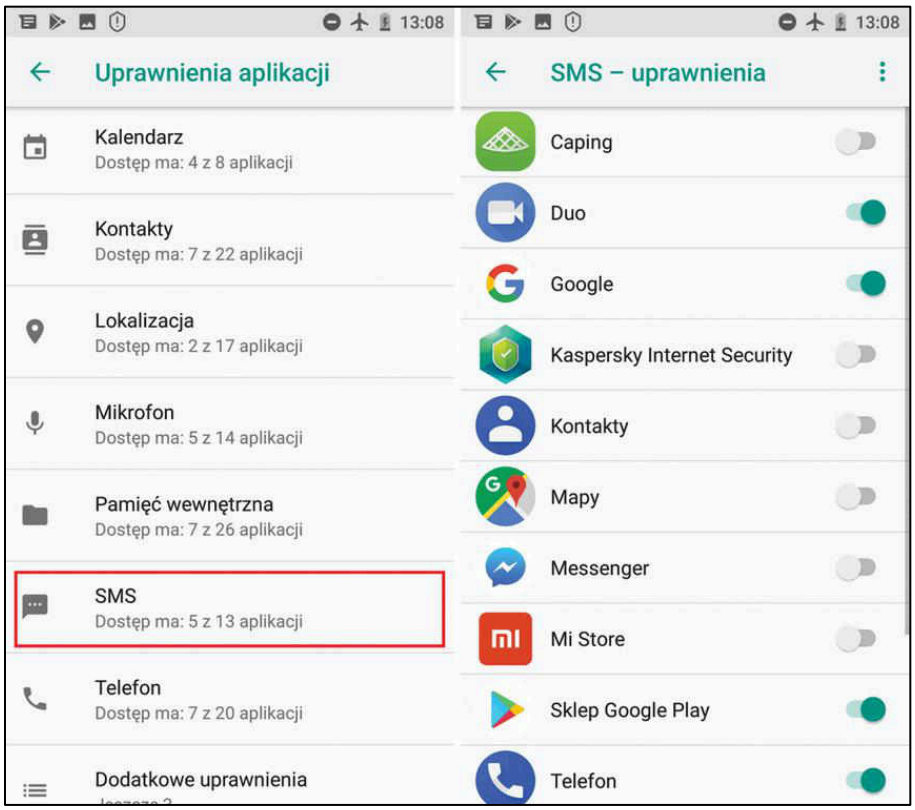
## Zabezpieczenie telefonu komórkowego

Smartfon to urządzenie, które mamy zawsze przy sobie, przez co jest on szczególnie narażony na zgubienie, kradzież lub ataki w przestrzeni publicznej. Aby odpowiednio zabezpieczyć swój telefon, należy przestrzegać następujących zasad:

- **Blokada ekranu:** Stosuj kody blokady zawierające co najmniej 8 znaków lub korzystaj z haseł alfanumerycznych. Zwykły, popularny czterocyfrowy PIN (taki jak data urodzenia czy proste "1234") to zdecydowanie za mało. Dłuższy ciąg znaków sprawia, że jego wzrokowe zapamiętanie przez osobę z boku jest w zasadzie niemożliwe. Zaleca się również zrezygnowanie z graficznych wzorów blokady (tzw. „wężyków"). Powierzchnia wyświetlacza łatwo zbiera zabrudzenia, a pozostawiony na niej ślad palca wskazuje kształt wzoru, co obniża poziom bezpieczeństwa urządzenia.
- **Biometria:** Warto na co dzień korzystać z nowoczesnych metod uwierzytelniania, takich jak rozpoznawanie twarzy (FaceID) lub czytniki linii papilarnych. Zabezpieczenia biometryczne są nie tylko znacznie wygodniejsze i szybsze niż każdorazowe wpisywanie długiego pinu, ale przede wszystkim o wiele trudniejsze do złamania. Ponadto, unikalny odcisk palca czy rysy twarzy są w codziennych warunkach praktycznie niemożliwe do podrobienia, co stanowi doskonałą barierę chroniącą prywatność.

**Higiena aplikacji i bezpieczne pobieranie:** Regularnie weryfikuj uprawnienia przyznawane aplikacjom na Twoim telefonie. Zastanów się, czy dana aplikacja faktycznie potrzebuje konkretnych funkcji do działania – na przykład: zwykły kalkulator nie potrzebuje dostępu do Twojej lokalizacji, mikrofonu ani książki adresowej. Ponadto, nie pobieraj aplikacji z nieznanych, nieoficjalnych źródeł (np. klikając w linki pobierania z podejrzanych SMS-ów czy reklam w internecie). Instaluj aplikacje **wyłącznie z oficjalnych sklepów z aplikacjami**, które posiadają wbudowane mechanizmy skanujące programy pod kątem wirusów. W zależności od tego, jakiej marki masz telefon, szukaj w menu następujących ikon:

- **Sklep Play (Google Play)** – jedyne oficjalne źródło aplikacji dla telefonów z systemem Android (czyli większości smartfonów na rynku, np. marek Samsung, Xiaomi, Motorola, Sony, Oppo).
- **App Store** – oficjalny sklep dedykowany wyłącznie dla urządzeń firmy Apple (iPhone, iPad).
- **AppGallery** – oficjalny sklep na nowszych telefonach marki Huawei (które nie posiadają dostępu do usług Google).




## Publiczne sieci Wi-Fi i ładowanie w miejscach publicznych

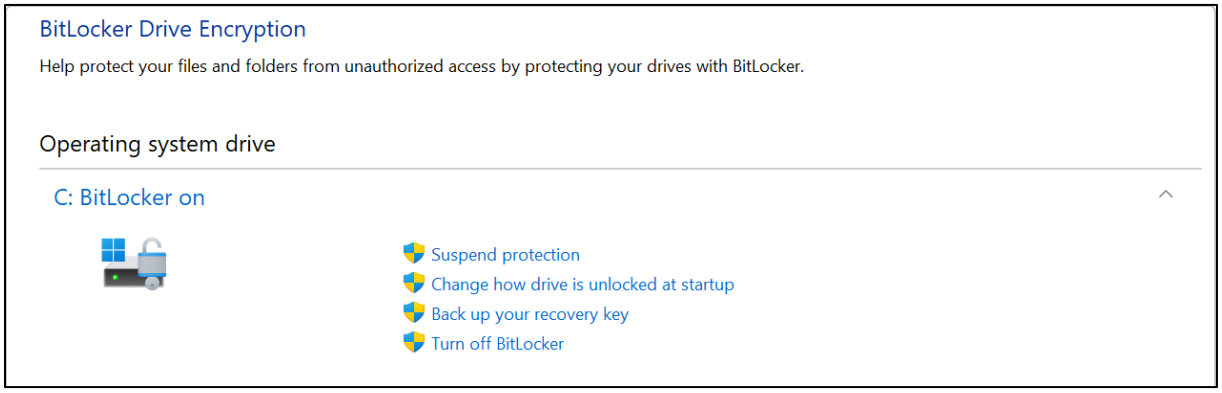
Przestrzeń publiczna, w tym komunikacja miejska czy centra handlowe, niesie ze sobą specyficzne zagrożenia dla naszych urządzeń mobilnych:

- **Publiczne sieci Wi-Fi:** Unikaj łączenia się z darmowymi, ogólnodostępnymi sieciami Wi-Fi (np. w kawiarniach, pociągach czy hotelach), ponieważ mogą one posłużyć przestępcom do przechwytywania wrażliwych danych. W niezabezpieczonej sieci dane krążą w sposób jawny, co pozwala osobom postronnym na ich potajemne kopiowanie i odczytywanie w locie. Zawsze bezpieczniejszym wyborem będzie skorzystanie z własnego internetu mobilnego od operatora.
- **Niebezpieczne stacje ładowania:** Nie ładuj telefonu w galeriach handlowych, pociągach czy na lotniskach, korzystając z ogólnodostępnych portów USB. Należy pamiętać, że ten sam kabel, który dostarcza prąd, służy jednocześnie do szybkiego przesyłania informacji. Cyberprzestępcy potrafią tak zmodyfikować publiczne stacje ładowania, że po podłączeniu telefonu złośliwy mechanizm w ułamku sekundy skopiuje prywatne dane lub zainstaluje wirusa. Najbezpieczniejszym nawykiem jest podłączanie własnej, tradycyjnej ładowarki do zwykłego gniazdka elektrycznego lub noszenie przy sobie osobistego powerbank'a.

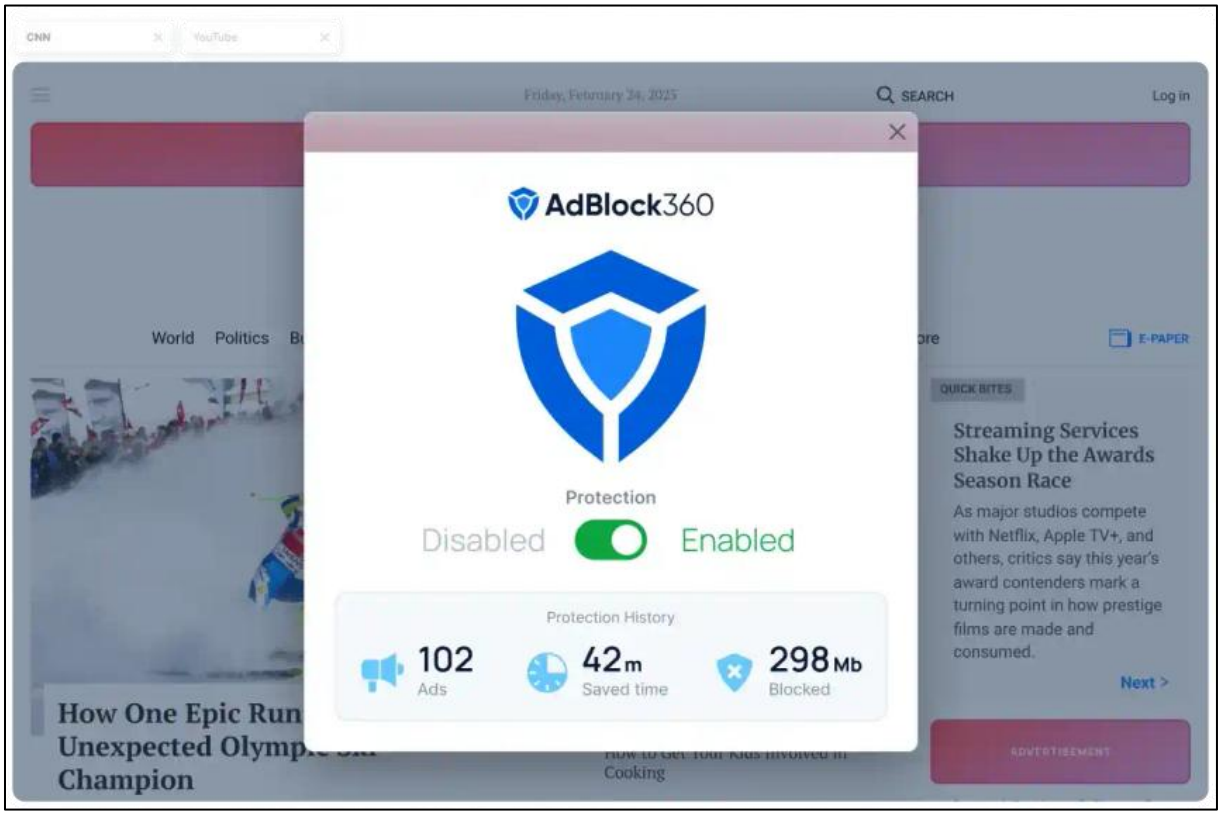
## Zabezpieczenie komputera

Komputery osobiste i służbowe często dają dostęp do najważniejszych dokumentów oraz systemów. Ich odpowiednie zabezpieczenie powinno być priorytetem:

- **Szyfrowanie dysku:** Zaszyfruj dysk twardy komputera za pomocą narzędzia Bitlocker. Należy bezwzględnie pamiętać, aby klucz odzyskiwania zapisać w bezpiecznym i niedostępnym dla osób trzecich miejscu.




**Ochrona podczas przeglądania:** Korzystaj z rozszerzeń blokujących złośliwe reklamy i skrypty, takich jak Adblock. Niektóre przeglądarki internetowe jak Brave posiadają już wbudowane opcje blokowania skryptów śledzących i reklam.




**Aktualizacje telefonu i komputera:** Regularnie instaluj aktualizacje systemu na obu urządzeniach, ponieważ usuwają one znane luki bezpieczeństwa. Szczegółowe zalecenia dotyczące aktualizowania systemu i aplikacji znajdziesz w rozdziale 9.

## Zagrożenia fizyczne: Nieznane nośniki USB

Jednym z najczęstszych wektorów ataków, wykorzystującym ludzką ciekawość, są podrzucone urządzenia USB.

- Nigdy, pod żadnym pozorem nie podłączaj do swojego komputera urządzeń USB, które zostały gdzieś znalezione. Warto pamiętać, że cyberprzestępcy celowo podrzucają takie "przynęty", a niebezpieczeństwo nie dotyczy tylko zwykłych pendrive'ów. Po podłączeniu do gniazda takie urządzenie może w ułamku sekundy zainstalować wirusa, który wykradnie hasła i pliki.
- Zagrożenie nie dotyczy wyłącznie pendrive'ów, na których może znajdować się złośliwe oprogramowanie. Należy unikać podłączania jakichkolwiek znalezionych gadżetów, takich jak wiatraczki USB czy przewody USB z końcówką do ładowania telefonu. Mogą one zostać specjalnie zmodyfikowane w celu uszkodzenia sprzętu lub wstrzyknięcia złośliwego kodu.

# Rozdział 8. Co zrobić po włamaniu na E-dziennik lub maila służbowego?

Włamanie na konto służbowe, takie jak szkolny E-dziennik czy skrzynka e-mail, w ręce przestępców mogą trafić niezwykle wrażliwe informacje, takie jak: adresy e-mail, poufna korespondencja, dokumenty placówki oraz dane osobowe uczniów i rodziców (w tym np. numery PESEL). W świetle obowiązującego prawa, a w szczególności na mocy Ogólnego rozporządzenia o ochronie danych (RODO) oraz Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, taka sytuacja stanowi poważny incydent teleinformatyczny oraz naruszenie ochrony danych osobowych to sytuacja kryzysowa. Aby zminimalizować negatywne skutki i uniknąć poważnych nieprzyjemności, należy działać szybko i metodycznie. Oto kroki, które należy podjąć natychmiast po wykryciu włamania:

## Kogo powiadomić i dlaczego to takie ważne?

Natychmiast powiadomić dyrektora szkoły – to obowiązek każdego pracownika, który uzyska informację o incydencie. Zgłoszenie może być telefoniczne, ale powinno zostać potwierdzone notatką służbową zawierającą:

- imię i nazwisko zgłaszającego,
- datę i godzinę wykrycia,
- miejsce (który system, komputer, konto),
- opis tego, co zostało zauważone.

Zabezpieczyć ślady w miarę możliwości zrobić zrzuty ekranu, nie kasować logów, nie „naprawiać" systemu. Każda ingerencja może zniszczyć dowody.

**Podejrzenie przejęcia konta:** Jeśli podałeś hasło na fałszywej stronie lub zauważyłeś nieautoryzowane logowanie, zmień hasło z innego, zaufanego urządzenia i zakończ pozostałe aktywne sesje. Jeżeli nie możesz tego zrobić samodzielnie, niezwłocznie poproś administratora o zablokowanie konta lub pomoc w odzyskaniu dostępu.

**Podejrzenie infekcji urządzenia:** Jeżeli uruchomiłeś podejrzany plik lub polecenie, odłącz komputer od Wi-Fi i wypnij przewód sieciowy. Wstrzymaj korzystanie z tego urządzenia i niezwłocznie skontaktuj się z administratorem IT, np. telefonicznie.

**Dalsze działania techniczne:** Nie usuwaj podejrzanych plików, nie kasuj logów, nie instaluj programów naprawczych i nie przeinstalowuj systemu. Diagnozę oraz usunięcie zagrożenia pozostaw administratorowi IT.

Współpraca z administracją IT / IOD – dyrektor przekazuje sprawę administratorowi systemów oraz Inspektorowi Ochrony Danych (IOD), który ocenia, czy doszło do naruszenia ochrony danych osobowych.

Informacje o zgłaszaniu incydentów do instytucji zewnętrznych znajdziesz w rozdziale 11 „Zgłaszanie incydentów”.

Rolą nauczyciela jest szybkie zgłoszenie incydentu, zabezpieczenie dostępnych śladów oraz wykonanie opisanych wyżej podstawowych działań ograniczających zagrożenie, zgodnie ze szkolną procedurą reagowania na incydenty. Dyrektor koordynuje reakcję szkoły, administrator IT prowadzi działania techniczne, a IOD wspiera ocenę naruszenia ochrony danych osobowych i obowiązków związanych z dalszym zgłoszeniem.

# Rozdział 9. Jak uniknąć złośliwego oprogramowania

Załącznik od rodzica, materiały do lekcji znalezione w internecie czy wiadomość z prośbą o aktualizację dziennika elektronicznego mogą wyglądać zwyczajnie. Każda z tych sytuacji wymaga jednak krótkiego sprawdzenia, zanim otworzysz plik, zainstalujesz program lub podasz hasło.

Ochronę przed złośliwym oprogramowaniem warto zacząć od ustalenia, skąd pochodzi otrzymana treść i czy rzeczywiście jej oczekujesz. Pomagają w tym sprawdzanie adresów stron, kontrolowanie rodzaju plików oraz działający antywirus.

## Czym jest złośliwe oprogramowanie?

Złośliwe oprogramowanie, nazywane również **malware**, to programy tworzone po to, aby szkodzić użytkownikowi lub działać na jego urządzeniu bez uprawnienia. Mogą wykradać hasła i dokumenty, przejmować dostęp do kont albo szyfrować pliki i żądać pieniędzy za ich odzyskanie. Ten ostatni rodzaj zagrożenia jest określany jako **ransomware**.

Nie każda infekcja powoduje widoczne problemy. Komputer może nadal działać normalnie, podczas gdy szkodliwy program zbiera informacje w tle. Dlatego brak nietypowych objawów nie jest potwierdzeniem bezpieczeństwa.

W pracy nauczyciela skutki infekcji mogą dotyczyć również danych uczniów i rodziców, materiałów dydaktycznych oraz dostępu do szkolnej poczty. Sprawdzaj otrzymane treści przed ich otwarciem, także wtedy, gdy wiadomość sprawia wrażenie służbowej.

**Niebezpieczne linki.** Link może prowadzić do strony pobierającej szkodliwy program, fałszywego formularza logowania albo instrukcji nakłaniającej do niebezpiecznej czynności. Strona wyłudzająca hasło nie musi niczego instalować na komputerze, aby spowodować szkodę.

**Uważaj na fałszywe testy CAPTCHA.** Strona może polecić użycie skrótu Windows + R, wklejenie „kodu weryfikacyjnego” i naciśnięcie Enter. Takie polecenie może uruchomić szkodliwy program. Prawdziwa CAPTCHA nie wymaga wykonywania poleceń w oknie Uruchom, Terminalu ani PowerShellu. Zamknij stronę, która tego żąda.

## Podejrzane pliki i załączniki

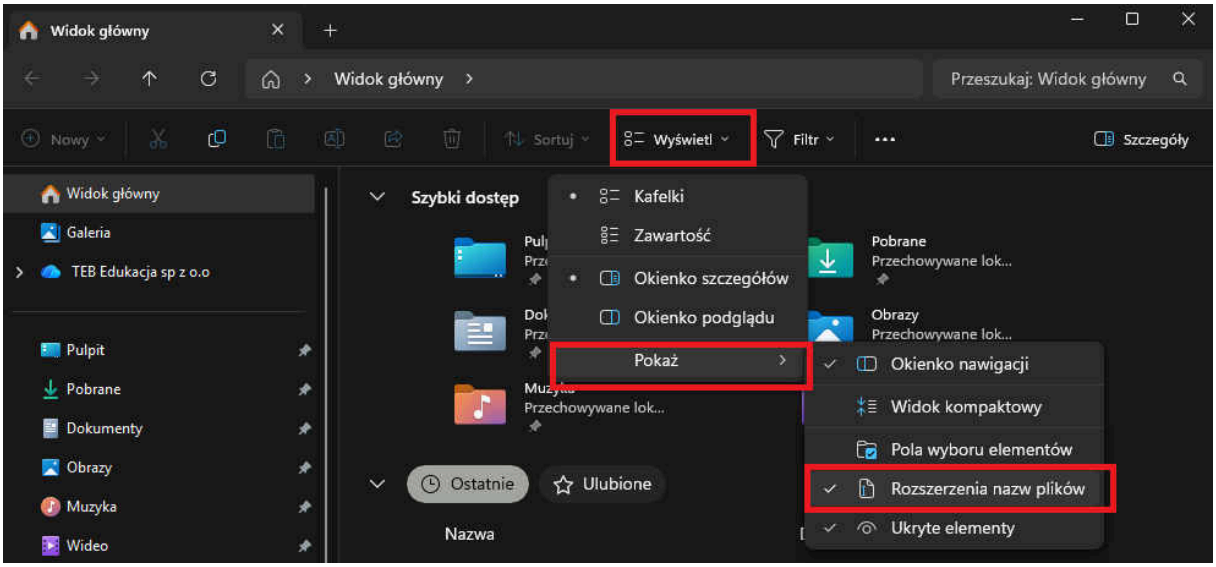
Przed otwarciem pliku sprawdź jego pochodzenie i pełną nazwę. Wiadomość od znajomej osoby także może być niebezpieczna, jeśli ktoś przejął jej konto lub podszył się pod nadawcę. Gdy nie oczekujesz załącznika, potwierdź jego wysłanie.

### Włącz wyświetlanie rozszerzeń plików

Rozszerzenie to końcowa część nazwy pliku, np. .pdf lub .docx. Pomaga rozpoznać jego deklarowany rodzaj. W Windows 11 włączysz jego wyświetlanie następująco:

1. Otwórz Eksplorator plików skrótem **Windows + E**.
2. Wybierz **Wyświetl**, następnie **Pokaż**.

3. Zaznacz **Rozszerzenia nazw plików**.




Nazwa plan_lekcji.pdf.exe kończy się rozszerzeniem **.exe**, więc wskazuje na program wykonywalny. Nie jest zwykłym dokumentem PDF. Sama ikona dokumentu może wprowadzać w błąd. Zmiana nazwy na plan_lekcji.pdf nie zamienia programu w bezpieczny dokument.

| **Rodzaj pliku** | **Na co zwrócić uwagę** |
|---|---|
| .exe, .msi | Program lub instalator. Nie uruchamiaj go jako rzekomego sprawdzianu, faktury czy planu lekcji. |
| .js, .vbs, .bat, .cmd, .ps1 | Skrypt mogący wykonywać polecenia. Nie uruchamiaj nieoczekiwanych skryptów z wiadomości. |
| .lnk | Skrót, który może uruchamiać program lub polecenie. Może udawać dokument. |
| .docm, .xlsm | Dokumenty obsługujące makra. Nie włączaj makr na prośbę niezweryfikowanego nadawcy. |
| .zip, .rar, .7z | Archiwa zawierające inne pliki. Oceń także ich zawartość; hasło do archiwum nie świadczy o bezpieczeństwie. |
| .pdf, .docx, .xlsx | Typowe dokumenty również mogą zawierać niebezpieczne odnośniki lub treści wykorzystujące błędy w aplikacjach, natomiast zdarza się to stosunkowo rzadko. |

Rozszerzenie jest wskazówką. Nie stanowi pełnej analizy zawartości pliku. Jeżeli dokument prosi o włączenie makr, wyłączenie antywirusa lub uruchomienie dodatkowego instalatora, przerwij działanie i wyjaśnij sytuację z nadawcą albo szkolnym informatykiem. Nie obchodź zabezpieczeń tylko po to, aby zobaczyć zawartość załącznika.

## Sprawdzanie linku w VirusTotal

VirusTotal to serwis zbierający wyniki analizy plików i adresów z wielu narzędzi bezpieczeństwa. Może pomóc ocenić otrzymaną treść, ale nie daje gwarancji jej bezpieczeństwa.

**Przed przesłaniem adresu zadbaj o poufność.** W standardowej usłudze zgłoszenia i informacje o nich mogą być udostępniane partnerom oraz uprawnionym klientom serwisu. Nie przesyłaj linków do resetowania hasła, zaproszeń dających dostęp do prywatnych materiałów ani adresów zawierających dane uczniów lub kody dostępu.

Link, który nie zawiera poufnych informacji, sprawdzisz następująco:

1. Kliknij go prawym przyciskiem myszy i wybierz opcję kopiowania adresu linku. Nie otwieraj strony, aby uzyskać jej adres.
2. Otwórz samodzielnie stronę https://www.virustotal.com/.
3. Wybierz zakładkę **URL**.
4. Wklej skopiowany adres do pola i zatwierdź sprawdzenie.
5. Poczekaj na raport. Odczytaj liczbę wykryć oraz datę ostatniej analizy.
6. Jeśli raport jest stary, możesz użyć dostępnej funkcji ponownej analizy, zwykle oznaczonej **Reanalyze**.

Nazwy przycisków mogą zależeć od wersji interfejsu i języka przeglądarki. Zwracaj uwagę, czy sprawdzasz właściwy adres.

Jeżeli nie możesz przesłać pełnego linku z powodu jego poufności, poproś informatyka o weryfikację. Wynik dotyczący samej domeny nie rozstrzyga, czy konkretny dokument, odnośnik lub formularz jest bezpieczny.

## Sprawdzanie pliku w VirusTotal

**Do standardowego VirusTotal nie przesyłaj dokumentacji szkolnej ani prywatnych dokumentów.** Dotyczy to m.in. list uczniów, ocen, opinii, orzeczeń, umów oraz korespondencji z rodzicami. Przesłanie pliku do analizy oznacza przekazanie jego zawartości zewnętrznemu serwisowi. Poufny załącznik sprawdź narzędziem zatwierdzonym przez placówkę lub przekaż do oceny osobie odpowiedzialnej za IT.

Jeżeli plik nie zawiera informacji poufnych i możesz go przekazać do tej usługi:

1. Pozostaw go nieotwarty. Nie pobieraj dodatkowych podejrzanych plików tylko po to, aby je testować.
2. Otwórz https://www.virustotal.com/ i wybierz zakładkę **File**.
3. Kliknij **Choose file** i wskaż plik na komputerze.
4. Potwierdź przesłanie, jeśli serwis o to poprosi.

5. Poczekaj na zakończenie analizy lub wyświetlenie istniejącego raportu.
6. Sprawdź liczbę wykryć, datę analizy oraz komunikaty poszczególnych narzędzi.

Przesłanie pliku przez formularz nie wymaga uruchamiania go na Twoim komputerze. Nie wyłączaj ochrony, jeśli antywirus zablokuje dostęp do pliku lub umieści go w kwarantannie. Taka blokada jest powodem do wyjaśnienia sprawy, a nie przeszkodą, którą należy obejść.

Sprawdzenie adresu strony i analiza pliku to różne czynności. Raport dotyczący linku nie zastępuje sprawdzenia pobranego załącznika.

**Jak odczytać wyniki analizy?**

| Wynik lub komunikat | Jak go rozumieć |
|---|---|
| **0/70** | W tym raporcie żadne z 70 narzędzi nie oznaczyło badanego elementu jako szkodliwego. Nie jest to gwarancja bezpieczeństwa. |
| **1/70** | Jedno narzędzie zgłosiło zagrożenie. Może to być błędny alarm albo wykrycie, którego inne narzędzia jeszcze nie potwierdziły. |
| **Wiele wykryć** | To silny sygnał ostrzegawczy. Wstrzymaj otwieranie pliku lub odwiedzanie strony i poproś o weryfikację. |
| **Undetected** | Dane narzędzie nie wykryło zagrożenia. Nie oznacza to potwierdzenia, że plik jest bezpieczny. |
| **Suspicious lub Malicious** | Narzędzie uznało element za podejrzany lub szkodliwy. |
| **Timeout lub brak obsługi typu pliku** | Narzędzie nie dostarczyło rozstrzygającego wyniku. Nie licz tego jako potwierdzenia bezpieczeństwa. |

Odczytuj raport razem z informacją o pochodzeniu pliku lub linku. Nowe zagrożenie może nie zostać jeszcze rozpoznane. Nie istnieje prosty próg liczby wykryć, poniżej którego każdy plik można bezpiecznie uruchomić. Błędne alarmy także się zdarzają i wymagają wyjaśnienia.

## Antywirus i ochrona w Windows 11

Antywirus monitoruje urządzenie i pomaga wykrywać oraz blokować złośliwe oprogramowanie. Windows 11 zawiera program antywirusowy **Microsoft Defender**, obsługiwany w aplikacji **Zabezpieczenia Windows**. Nie trzeba instalować kolejnego programu tylko dlatego, że ochrona wbudowana jest dostępna bez dodatkowej opłaty. Na szkolnym komputerze korzystaj z rozwiązania przyjętego przez placówkę.

Nie instaluj równocześnie kilku niezależnych antywirusów z aktywną ochroną w czasie rzeczywistym. Mogą się wzajemnie zakłócać i powodować problemy z działaniem ochrony lub wydajnością komputera.

**Przeskanuj konkretny plik**

1. Odszukaj plik w Eksploratorze, bez jego otwierania.
2. Kliknij go prawym przyciskiem myszy.
3. W Windows 11 wybierz **Pokaż więcej opcji**, jeśli polecenia skanowania nie widać od razu.
4. Wybierz **Skanuj za pomocą Microsoft Defender** i poczekaj na wynik. Jeśli używasz innego antywirusa, skorzystaj z jego odpowiedniej funkcji.

**Co zrobić po otwarciu podejrzanej treści**

Samo wyświetlenie strony nie przesądza o infekcji. Istotne jest, czy uruchomiono plik, wykonano polecenie, zainstalowano program albo wpisano hasło.

Jeżeli uruchomiłeś podejrzany plik lub polecenie, odłącz komputer od Wi-Fi i sieci przewodowej. Na sprzęcie szkolnym od razu zgłoś sytuację informatykowi i opisz wykonane czynności. Nie przesyłaj podejrzanego załącznika kolejnym osobom. Zachowaj wiadomość i zanotuj godzinę zdarzenia.

Jeśli wpisałeś hasło na podejrzanej stronie, zmień je z innego, zaufanego urządzenia. Zakończ pozostałe sesje konta i włącz uwierzytelnianie wieloskładnikowe. W przypadku konta służbowego powiadom osobę odpowiedzialną za jego obsługę. Sama zmiana hasła nie usuwa ewentualnego złośliwego programu z komputera.

Po podejrzeniu infekcji nie uznawaj jednego skanowania bez wykryć za dowód, że urządzenie można ponownie bezpiecznie wykorzystywać do pracy z danymi uczniów. Dalsze czynności ustal z informatykiem.

## Nawyki ograniczające ryzyko

**Aktualizuj system i aplikacje.** Poprawki bezpieczeństwa dotyczą także przeglądarki, pakietu biurowego oraz czytnika PDF. Korzystaj z oprogramowania objętego wsparciem producenta.

**Pobieraj programy z oficjalnych źródeł.** Unikaj pirackich wersji, aktywatorów i „naprawiaczy” wymagających wyłączenia ochrony. Aktualizacje uruchamiaj z ustawień programu lub systemu, a nie z przypadkowego okna na stronie.

**Dbaj o kopie zapasowe.** Korzystaj ze sposobu przyjętego przez szkołę. Kopia na dysku stale podłączonym do komputera również może zostać zaszyfrowana. Przynajmniej jedna kopia powinna być odłączona albo chroniona przed zmianą i usunięciem z konta używanego na komputerze. Sprawdzaj, czy pliki można z niej odtworzyć.

# Rozdział 10. Zabezpieczanie dowodów cyfrowych

W sytuacji wystąpienia cyberprzemocy rola nauczyciela nie kończy się na udzieleniu wsparcia psychologicznego. Równie kluczowe jest natychmiastowe i metodyczne zabezpieczenie śladów. Właściwie zgromadzone materiały stanowią jedyną obiektywną podstawę do wyciągnięcia konsekwencji regulaminowych wobec sprawcy, a w skrajnych przypadkach – do interwencji organów ścigania.

**Jak prawidłowo gromadzić dowody**

Zwykły zrzut ekranu choć ważny w takich sytuacjach to wycięty z kontekstu jest bardzo łatwy do podważenia lub sfałszowania za pomocą prostych programów graficznych bądź algorytmów sztucznej inteligencji. Aby dowód cyfrowy miał wartość merytoryczną i prawną, musi zawierać metadane i szerszy kontekst zaistniałej sytuacji.

- **Stosuj zasadę „czworga oczu”:** W miarę możliwości zabezpieczanie dowodów (np. przeglądanie wiadomości na telefonie ucznia i robienie zdjęć/zrzutów) powinno odbywać się w obecności drugiego pracownika szkoły (innego nauczyciela lub pedagoga). Zabezpiecza to osobę interweniującą przed ewentualnymi oskarżeniami o naruszenie prywatności czy modyfikację danych na urządzeniu ucznia.

- **Kopiuj i zachowuj adresy URL (linki):** Zawsze kopiuj dokładny adres strony internetowej lub profilu w mediach społecznościowych, na którym doszło do ataku. Zapisz go w dokumencie tekstowym wraz z datą i godziną odkrycia treści.

- **Zabezpieczaj profil sprawcy:** Zrób zrzuty ekranu profilu sprawcy (nawet jeśli jest to konto anonimowe/fikcyjne). Zwróć uwagę na nazwę użytkownika, jeśli jest dostępny numer ID, opis profilu, oraz wszystkie inne informacje o koncie które są widoczne.

- **Zapisuj strony jako pliki PDF:** Zamiast robić dziesiątki zrzutów ekranu długiej dyskusji, skorzystaj z opcji „Drukuj” w przeglądarce i wybierz „Zapisz jako PDF”. Pozwoli to zachować oryginalny układ strony, klikalne linki oraz kontekst całej konwersacji.

- **Zabezpieczanie wiadomości e-mail:** Nigdy nie usuwaj obraźliwych wiadomości. Oprócz treści samej wiadomości, kluczowy jest tzw. nagłówek e-maila zawierający m.in. adres nadawcy. W programach pocztowych szukaj opcji „Pokaż oryginał” lub „Wyświetl źródło wiadomości” i zapisz całość w pliku tekstowym.

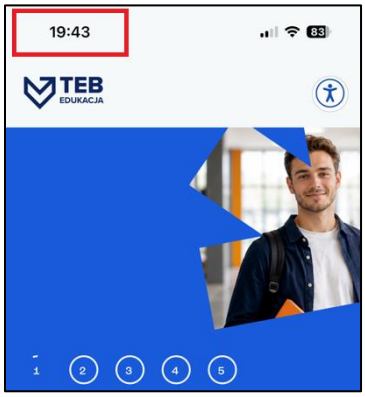
- **Nagrywaj ekran w przypadku multimediów:** Jeśli cyberprzemoc ma formę znikających relacji (np. Instastories, Snapchat), transmisji na żywo lub wiadomości głosowych, użyj funkcji nagrywania ekranu z włączonym dźwiękiem.

- **Nie blokuj sprawcy przed zebraniem dowodów:** Zablokowanie użytkownika w niektórych przypadkach powoduje zniknięcie całej historii konwersacji na danym urządzeniu. Najpierw zabezpiecz materiały, dopiero potem zablokuj kontakt.

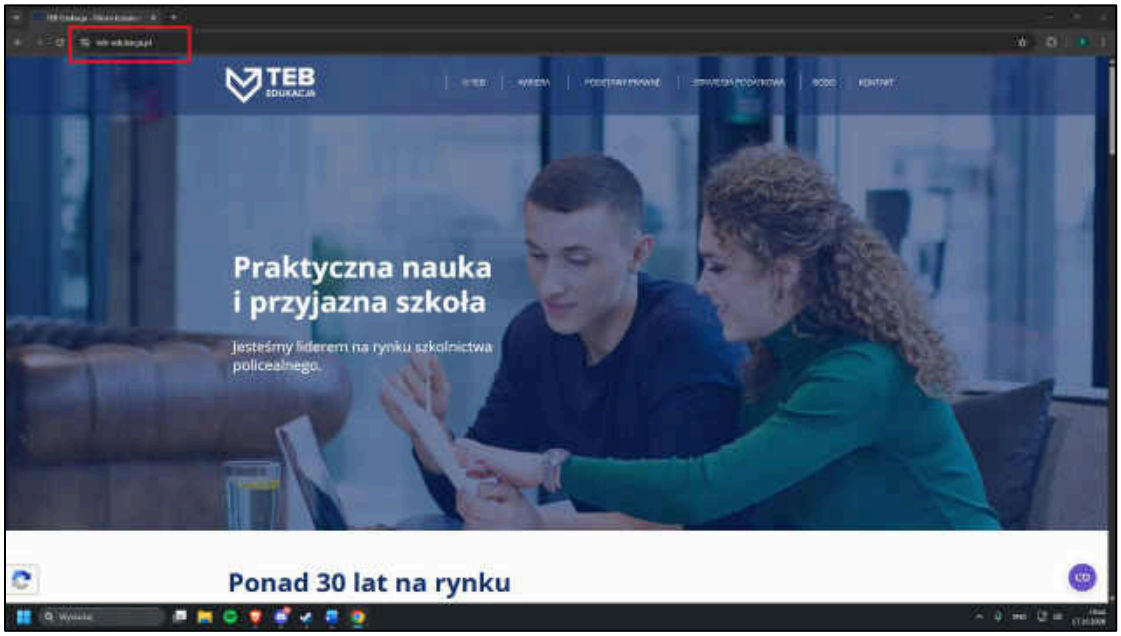
## Jak poprawnie wykonywać zrzuty ekranu

Aby zrzut ekranu (tzw. screen) stanowił wiarygodny dowód, musi ukazywać pełny kontekst sytuacji i nie nosić śladów żadnych modyfikacji.

- **Zawsze chwytaj pełny ekran:** Unikaj wycinania tylko samego fragmentu z obraźliwą wiadomością. Zrzut musi obejmować cały monitor lub ekran telefonu.
- **Uwidocznij datę i godzinę:** Na komputerze upewnij się, że widoczny jest pasek zadań z zegarem systemowym. Na telefonie – górna belka z godziną.




- **Zadbaj o widoczność adresu (URL):** Jeśli dowód znajduje się na stronie internetowej, pasek adresu przeglądarki z dokładnym linkiem musi być w pełni widoczny.



- **Nie modyfikuj oryginału:** Nie zamazuj danych, nie dodawaj czerwonych strzałek ani podkreśleń na pierwotnym pliku. Jeśli musisz coś zaznaczyć dla dyrekcji lub pedagoga, zrób to wyłącznie na kopii pliku.

## Metody zapisu zrzutów ekranu - komputery z systemem Windows:

- **Metoda 1: Automatyczny zapis** Naciśnij jednocześnie klawisz z **logo Windows + PrtScn** (Print Screen). Ekran na ułamek sekundy przygaśnie, a gotowy plik graficzny (obejmujący cały widok) zostanie automatycznie zapisany w folderze *Ten komputer -> Obrazy -> Zrzuty ekranu*.

- **Metoda 2: Narzędzie Wycinanie** Naciśnij skrót **Win + Shift + S**. Ekran zszarzeje. Na małym pasku, który pojawi się u góry ekranu, wybierz ostatnią ikonę z prawej strony (**Zrzut pełnego ekranu**). Obraz zapisze się w pamięci (schowku) – musisz otworzyć program (np. Word lub Paint), wkleić go za pomocą skrótu **Ctrl + V** i zapisać plik.

- **Metoda 3: Tradycyjny klawisz PrtScn** Wciśnięcie samego klawisza **PrtScn** (na niektórych klawiaturach *PrtSc/SysRq*) kopiuje widok całego ekranu. Następnie należy otworzyć edytor tekstu (Word) lub graficzny (Paint), wkleić obraz (Ctrl + V) i zapisać dokument.

## Metody zapisu zrzutów ekranu - Urządzenia mobilne (smartfony i tablety):

- **Telefony z systemem Android (np. Samsung, Xiaomi, Motorola):** Naciśnij i przytrzymaj jednocześnie przycisk Zmniejszania głośności oraz przycisk Zasilania (Blokady) przez około sekundę. Plik zostanie zapisany w galerii telefonu w folderze *Zrzuty ekranu* lub *Screenshots*.

- **iPhone (Apple) z Face ID (bez okrągłego przycisku pod ekranem):** Naciśnij jednocześnie przycisk Boczny (z prawej strony obudowy) oraz przycisk Zwiększania głośności (z lewej), a następnie szybko je puść.

- **iPhone z przyciskiem Początek (starsze modele z Touch ID):** Naciśnij jednocześnie przycisk **Boczny/Górny** oraz okrągły przycisk **Początek** pod ekranem.

## Metody nagrywania ekranu - Urządzenia mobilne (smartfony i tablety) – opcje wbudowane.

Telefony z systemem Android (np. Samsung, Xiaomi, Motorola):

- Rozwiń górne menu (panel szybkich ustawień), przeciągając palcem z góry ekranu w dół.

- Znajdź ikonę Nagrywanie ekranu (lub *Rejestrator ekranu*). Jeśli jej tam nie ma, przesuń w lewo na kolejne strony lub dodaj ją z menu edycji (ikona ołówka).
- Po kliknięciu wybierz opcję nagrywania dźwięków ("Dźwięki multimediów" lub "Systemowe").
- Rozpocznie się krótkie odliczanie. Aby zakończyć, ponownie opuść panel i kliknij przycisk "Zatrzymaj". Plik wideo zapisze się w Galerii.

Telefony z systemem IOS (Apple):

- Otwórz Centrum sterowania (przesuń palcem w dół z prawego górnego rogu ekranu, a w starszych modelach – z dołu do góry).
- Stuknij ikonę Nagrywanie ekranu (szare kółko z kropką w środku).
- Jeśli chcesz nagrać również to, co mówisz (np. własny komentarz), naciśnij i przytrzymaj ikonę, a następnie włącz ikonę Mikrofonu.
- Po 3-sekundowym odliczaniu rozpocznie się nagrywanie (ikona zmieni kolor na czerwony). Aby zakończyć, stuknij czerwony pasek lub godzinę na górze ekranu i wybierz „Narzędzia” -> „Zatrzymaj”. Film znajdziesz w aplikacji Zdjęcia.

## Metody nagrywania ekranu - komputery z systemem Windows.

- Wciśnij skrót Win + Shift + S lub wyszukaj "Narzędzie Wycinanie" w menu Start.
- Na górnym pasku narzędzia zmień ikonę z aparatu (zrzut) na ikonę Kamery wideo.
- Zaznacz obszar ekranu, który chcesz nagrać (najlepiej zaznacz cały ekran).
- Kliknij przycisk Start na górze. Po zakończeniu kliknij czerwoną ikonę "Zatrzymaj", a następnie zapisz plik wideo na dysku (ikona dyskietki).

Alternatywnie:

- Wciśnij jednocześnie klawisze Win + G.
- W lewym górnym rogu w panelu "Rejestruj" kliknij ikonę kropki nagrywania (lub użyj skrótu Win + Alt + R).
- Aby upewnić się, że dźwięk jest nagrywany, w panelu "Dźwięk" sprawdź, czy suwaki systemowe nie są wyciszone.
- Aby zatrzymać, kliknij niebieski kwadrat na małym pasku pływającym. Filmy domyślnie zapisują się w folderze *Ten komputer -> Wideo -> Przechwycone*.

# Rozdział 11. Zgłaszanie incydentów

Skuteczna reakcja na cyberprzemoc wymaga od nauczyciela wiedzy o tym, do kogo skierować sprawę w zależności od wagi incydentu. Zgłaszanie takich sytuacji można podzielić na cztery główne obszary: środowisko szkolne, wsparcie specjalistyczne, administrację serwisów oraz organy ścigania.

## Wewnątrz struktur szkolnych i środowiska ucznia.

Pierwszym krokiem, o ile sytuacja nie zagraża bezpośrednio życiu i zdrowiu ucznia, jest uruchomienie procedur wewnątrzszkolnych.

- **Dyrektor szkoły, pedagog i psycholog szkolny:** Poinformuj ich o zaistniałej sytuacji. Dyrektor koordynuje działania szkoły i kontakt z odpowiednimi instytucjami zgodnie z przyjętymi procedurami. Pedagog i psycholog oceniają potrzeby poszkodowanego ucznia, zapewniają mu wsparcie oraz pomagają zaplanować działania wychowawcze wobec sprawcy, jeśli jest on uczniem tej samej szkoły.
- **Sporządź notatkę służbową:** Opisz rzeczowo przebieg zdarzenia. Wskaż datę i godzinę, osoby uczestniczące w zdarzeniu, świadków oraz podjęte działania. Wymień zabezpieczone materiały, np. wiadomości, zrzuty ekranu i adresy stron.
- **Złóż pisemne zgłoszenie dyrektorowi szkoły:** Przekaż opis incydentu wraz z notatką służbową i zabezpieczonymi materiałami, zgodnie z procedurą obowiązującą w placówce. Zachowaj kopię zgłoszenia i potwierdzenie jego przekazania.
- **Rodzice i opiekunowie prawni:** Należy poinformować zarówno rodziców poszkodowanego ucznia, jak i rodziców sprawcy jeśli jego tożsamość jest znana. Komunikacja powinna opierać się na faktach i zabezpieczonych dowodach (np. zrzutach ekranu), unikając stygmatyzacji.

## Instytucje i organizacje specjalistyczne.

W Polsce funkcjonują dedykowane zespoły reagujące na naruszenia w sieci, do których nauczyciel lub szkoła może zgłosić incydent oficjalną drogą elektroniczną.

- **Dyżurnet.pl (zespół NASK):** Przyjmuje zgłoszenia dotyczące nielegalnych treści w internecie, w tym materiałów przedstawiających seksualne wykorzystywanie dzieci, rasizm, ksenofobię czy drastyczną przemoc. Zgłoszenia można dokonać anonimowo.
- **CERT Polska (incydent.cert.pl):** Właściwy adres do zgłaszania incydentów zagrażających cyberbezpieczeństwu, takich jak kradzież kont na portalach społecznościowych, włamania na skrzynki e-mail czy fałszywe strony (phishing) wykorzystywane do nękania.
- **Prezes Urzędu Ochrony Danych Osobowych (UODO):** W przypadku naruszenia ochrony danych osobowych administrator danych, przy wsparciu IOD, ocenia konieczność zgłoszenia sprawy do UODO. Zgłoszenia dokonuje się bez zbędnej zwłoki, w miarę możliwości w ciągu 72 godzin od stwierdzenia naruszenia. Zgłoszenie nie jest wymagane,

jeżeli jest mało prawdopodobne, by naruszenie powodowało ryzyko dla praw lub wolności osób, których dane dotyczą.

- **Telefon 800 100 100** (Fundacja Dajemy Dzieciom Siłę): Bezpłatna infolinia dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci. Nauczyciel może tam skonsultować trudny przypadek cyberprzemocy i otrzymać wsparcie prawne oraz psychologiczne w zaplanowaniu interwencji.

## Administratorzy platform i serwisów społecznościowych

Większość aktów cyberprzemocy ma miejsce na zewnętrznych platformach (Instagram, TikTok, Snapchat, Discord, grupy na Messengerze). Nauczyciel, we współpracy z uczniem lub jego rodzicami, powinien zadbać o usunięcie szkodliwych treści.

- **Zgłoszenia wewnątrz aplikacji:** Należy korzystać z wbudowanych funkcji "Zgłoś" dostępnych przy konkretnych postach, komentarzach lub profilach. Powód zgłoszenia należy sklasyfikować jako "Nękanie i cyberprzemoc".
- **Formularze kontaktowe dla organów ścigania:** W przypadku poważnych przestępstw platformy posiadają specjalne kanały kontaktu, jednak korzysta z nich bezpośrednio policja, aby zabezpieczyć np. adresy IP logowania sprawcy.

## Organy ścigania i wymiar sprawiedliwości

Zgłoszenie na policję lub do sądu jest konieczne, gdy incydent wyczerpuje znamiona przestępstwa (np. groźby karalne, kradzież tożsamości, rozpowszechnianie intymnych zdjęć, uporczywe nękanie – stalking).

- **Policja (lokalna komenda lub Wydział do Walki z Cyberprzestępczością):** Zgłoszenia może dokonać dyrektor szkoły lub rodzice ofiary (nauczyciel zazwyczaj występuje w roli świadka). Policja dysponuje narzędziami pozwalającymi na ustalenie tożsamości anonimowych sprawców na podstawie adresów IP i logów z serwerów.
- **Sąd Rodzinny (Wydział Rodzinny i Nieletnich):** Jeśli sprawca cyberprzemocy ma od 13 do 17 lat i dopuszcza się czynów karalnych lub wykazuje silne przejawy demoralizacji, dyrektor szkoły ma obowiązek skierować zawiadomienie bezpośrednio do sądu rodzinnego, który podejmuje środki wychowawcze lub poprawcze.

# Rozdział 12. Aspekty prawne i tarcza ochronna nauczyciela

## Dlaczego mit „uczniowi nic nie można zrobić” to niebezpieczna fikcja?

W pokojach nauczycielskich często powtarza się przekonanie, że współczesna szkoła wiąże pedagogom ręce, a niepełnoletni uczeń w sieci i w klasie pozostaje całkowicie bezkarny. To jeden z najbardziej szkodliwych mitów w polskiej oświacie. Prawo nie kończy się przed drzwiami szkoły ani w momencie zalogowania się ucznia na TikToka, Discorda czy grupę klasową.

Nauczyciel nie jest bezbronnym obserwatorem. Polskie przepisy wyposażają go w silną ochronę prawną, a za ataki wymierzone w bezpieczeństwo szkoły, godność, prywatność czy wizerunek pedagoga grożą bardzo surowe konsekwencje – zarówno karne, jak i finansowe. Kluczem do skutecznej obrony jest jednak świadomość własnych praw oraz wiedza, które zachowania uczniów przestają być „głupim żartem”, a stają się czynem karalnym lub przestępstwem.

## Tarcza funkcjonariusza publicznego – jak prawo chroni nauczyciela?

Fundamentem bezpieczeństwa prawnego każdego pedagoga jest **art. 63 ust. 1 Karty Nauczyciela**. Przepis ten stanowi, że nauczyciel – **podczas lub w związku z pełnieniem obowiązków służbowych** – korzysta z ochrony przewidzianej dla **funkcjonariuszy publicznych** na zasadach określonych w Kodeksie karnym.

Co to oznacza w codziennej praktyce i dlaczego słowo „w związku” jest tu kluczowe? Ochrona ta nie działa wyłącznie w trakcie 45 minut lekcji przy tablicy. Działa również po dzwonku, w weekend czy w wakacje, jeżeli atak na nauczyciela (np. wyzwiska w internecie, groźby na ulicy, porysowanie samochodu czy opublikowanie kompromitującego fotomontażu) ma bezpośredni związek z pełnioną przez niego funkcją, wystawioną oceną lub uwagą wpisaną do e-dziennika.

Z tytułu tej szczególnej ochrony czyny wymierzone w nauczyciela są traktowane znacznie surowiej niż wobec przeciętnego obywatela i **ścigane są z urzędu** (przez Policję i prokuraturę, bez konieczności wnoszenia przez nauczyciela prywatnego aktu oskarżenia):

1. **Znieważenie nauczyciela (art. 226 § 1 Kodeksu karnego):** Ubliżanie nauczycielowi, wulgarne wyzwiska rzucone w klasie, obraźliwe komentarze na szkolnym czacie czy wyzywające wiadomości wysłane przez e-dziennik podlegają grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

2. **Naruszenie nietykalności cielesnej (art. 222 § 1 Kodeksu karnego):** Prawo chroni fizyczną nietykalność pedagoga jeszcze zanim dojdzie do jakiegokolwiek uszczerbku na zdrowiu. Odepchnięcie nauczyciela, szarpnięcie za ubranie, rzucenie w niego przedmiotem, oblanie wodą czy strącenie okularów to przestępstwo zagrożone karą do 3 lat pozbawienia wolności.

3. **Czynna napaść (art. 223 § 1 Kodeksu karnego):** Najpoważniejsza kategoria agresji fizycznej – działanie wspólnie i w porozumieniu z inną osobą lub z użyciem niebezpiecznego przedmiotu (np. noża, pałki, gazu lub środka obezwładniającego). Grozi za to od roku do aż 10 lat pozbawienia wolności.

4. **Wymuszanie czynności służbowych (art. 224 § 2 Kodeksu karnego):** Stosowanie przemocy lub groźby bezprawnej (przez ucznia lub agresywnego rodzica) w celu zmuszenia nauczyciela do zmiany oceny, cofnięcia uwagi, przepuszczenia do następnej klasy lub zaniechania zawiadomienia dyrekcji jest zagrożone karą do 3 lat więzienia.

5. **Obowiązek obrony z urzędu (art. 63 ust. 2 Karty Nauczyciela):** W sytuacji naruszenia powyższych praw nauczyciel nie powinien zostawać z problemem sam. Przepisy nakładają na **dyrektora szkoły oraz organ prowadzący** ustawowy obowiązek występowania z urzędu w obronie nauczyciela.

## Wykorzystanie wizerunku nauczyciela, memy, Deepfake i cyberprzemoc – co grozi uczniom?

Smartfon w rękach ucznia w kilka sekund może stać się narzędziem naruszającym dobra osobiste pedagoga. Nagrywanie nauczyciela z ukrycia podczas lekcji, robienie zdjęć z zaskoczenia, tworzenie wulgarnych memów czy wykorzystywanie generatorów sztucznej inteligencji (Deepfake) do nakładania twarzy nauczyciela na kompromitujące wideo lub klonowania jego głosu to zjawiska, które bezpośrednio uderzają w autorytet i godność zawodową.

Warto uświadamiać uczniów (oraz ich rodziców), że takie działania uruchamiają całą kaskadę konsekwencji prawnych:

1. **Bezprawne rozpowszechnianie wizerunku (art. 81 Prawa autorskiego oraz art. 23 i 24 Kodeksu cywilnego):** Wizerunek każdego człowieka jest prawnie chronionym dobrem osobistym. Nauczyciel w klasie nie jest „osobą powszechnie znaną" w rozumieniu przepisów medialnych – publikowanie jego zdjęć lub nagrań z lekcji na TikToku, Instagramie czy zamkniętych serwerach bez jego wyraźnej zgody jest nielegalne. Poszkodowany nauczyciel może żądać na drodze cywilnej nie tylko natychmiastowego usunięcia materiału i oficjalnych przeprosin, ale także **zadośćuczynienia finansowego lub wpłaty na cel społeczny** (co w przypadku niepełnoletnich sprawców bardzo często kończy się dotkliwym obciążeniem finansowym ich rodziców).

2. **Zniesławienie i pomówienie w sieci (art. 212 § 2 Kodeksu karnego):** Rozpowszechnianie nieprawdziwych lub zmanipulowanych informacji, które mogą poniżyć nauczyciela w opinii publicznej lub narazić go na utratę zaufania potrzebnego do wykonywania zawodu (np. sfabrykowane za pomocą AI nagranie głosowe lub wideo sugerujące nieetyczne zachowanie pedagoga), stanowi przestępstwo zagrożone karą do roku pozbawienia

wolności. Choć przestępstwo to jest co do zasady ścigane z oskarżenia prywatnego, nauczyciel – wspierany z urzędu przez dyrektora szkoły na mocy art. 63 ust. 2 Karty Nauczyciela – powinien złożyć do prokuratury wniosek o objęcie ścigania z urzędu ze względu na ważny interes społeczny (zgodnie z art. 60 § 1 Kodeksu postępowania karnego).

3. **Kradzież tożsamości i podszywanie się (art. 190a § 2 Kodeksu karnego):** Zakładanie fałszywych profili w mediach społecznościowych ze zdjęciem oraz imieniem i nazwiskiem nauczyciela, rozsyłanie z nich wiadomości do innych osób czy zamawianie niechcianych usług na dane pedagoga w celu wyrządzenia mu szkody osobistej lub majątkowej to przestępstwo zagrożone karą **od 6 miesięcy do 8 lat pozbawienia wolności**.

4. **Cyberstalking i uporczywe nękanie (art. 190a § 1 Kodeksu karnego):** Zorganizowane nękanie nauczyciela – np. głuche telefony w nocy, masowe wysyłanie wulgarnych wiadomości, publikowanie prywatnego adresu czy numeru telefonu w sieci, wzbudzające uzasadnione poczucie zagrożenia lub istotnie naruszające prywatność – również podlega karze od 6 miesięcy do 8 lat więzienia.

5. **Happy slapping – prowokacja pod kamerę:** Szczególnie niebezpiecznym zjawiskiem w szkołach jest tzw. *happy slapping*. Polega on na celowym sprowokowaniu nauczyciela (lub innego ucznia) do gwałtownej reakcji emocjonalnej albo fizycznej, nagraniu wyłącznie samego momentu wybuchu (z pominięciem wcześniejszej prowokacji) i opublikowaniu filmu w sieci. Takie działanie może łączyć w sobie znieważenie funkcjonariusza publicznego, zniesławienie oraz naruszenie dóbr osobistych.

6. **Frapping i włamania na konta (art. 267 Kodeksu karnego):** Jeśli uczeń wykorzysta moment nieuwagi na przerwie, usiądzie do niezablokowanego komputera nauczyciela lub przejmie jego sesję logowania, aby wpisać oceny w e-dzienniku albo opublikować ośmieszający post na jego profilu (tzw. *frapping*), popełnia przestępstwo bezprawnego uzyskania dostępu do informacji (do 2 lat pozbawienia wolności), a w przypadku zmiany danych w systemie informatycznym – przestępstwo z art. 268a Kodeksu karnego (do 3 lat pozbawienia wolności).

## Groźby w sieci i fałszywe alarmy – kiedy „internetowy challenge” kończy się aresztem?

Wydarzenia z października 2026 roku wstrząsnęły polską oświatą i bezpowrotnie zmieniły podejście służb do bezpieczeństwa w szkołach. Brutalne ataki z użyciem niebezpiecznych narzędzi w placówkach na Mazowszu – m.in. w **Ostrołęce** (gdzie 19-letni napastnik ranił nożem dziewięć osób, w tym uczniów i nauczycieli, mając przy sobie również domowej roboty materiał wybuchowy) oraz tragiczny w skutkach atak 15-latka w szkole w **Leszczydole-Nowinach**, w którym życie straciła pracownica szkoły, a rannych zostało dwoje

pedagogów – pokazały, że zagrożenie fizyczne bywa poprzedzone sygnałami w przestrzeni cyfrowej.

Tuż po tych tragediach przez polski internet przetoczyła się fala dezinformacji, sfabrykowanych list „szkół przeznaczonych do ataku", plotek o rzekomym internetowym wyzwaniu (*challenge'u*) oraz nagrań publikowanych przez nastolatków z nożami lub wygenerowanych przy użyciu sztucznej inteligencji. Efektem była gigantyczna operacja Policji i Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) – dziesiątki tysięcy skontrolowanych placówek i blisko dwustu zatrzymanych w ciągu zaledwie kilku dni.

W rozmowach z uczniami i podczas godzin wychowawczych należy bardzo wyraźnie podkreślać, że po ostatnich wydarzeniach służby stosują **zasadę zera tolerancji** dla jakichkolwiek gróźb czy „żartów" o zamachach:

1. **Fałszywy alarm i wywołanie paniki (art. 224a Kodeksu karnego):** To przepis, z którego najczęściej odpowiadają dziś autorzy „żartobliwych" zapowiedzi ataków na szkoły. Kto, wiedząc, że zagrożenie nie istnieje, stwarza sytuację mającą wywołać przekonanie o zagrożeniu życia lub zdrowia wielu osób i wywołuje tym reakcję służb (np. publikuje na TikToku nagranie z podpisem „Jutro krwawy piątek w naszym liceum" lub rozsyła fałszywą listę szkół, przez co do placówki wkracza Policja, a lekcje są odwoływane), podlega karze **od 6 miesięcy do 8 lat pozbawienia wolności**! Jeżeli sprawca wywoła więcej niż jedno takie zdarzenie, kara rośnie do przedziału **od 2 do aż 15 lat więzienia**. Nie ma przy tym żadnego znaczenia tłumaczenie, że „filmik wygenerowało AI", a autor „chciał tylko nabić zasięgi lub odwołać sprawdzian".

2. **Groźby karalne (art. 190 § 1 Kodeksu karnego):** Wysłanie nauczycielowi lub uczniowi wiadomości z groźbą pobicia, użycia noża czy pozbawienia życia (bądź wrzucenie zdjęcia z bronią i oznaczeniem konkretnej osoby), które wzbudza w adresacie uzasadnioną obawę, jest przestępstwem zagrożonym karą do 3 lat pozbawienia wolności.

3. **Publiczne nawoływanie do zbrodni lub pochwalanie przestępstwa (art. 255 § 1–3 Kodeksu karnego):** Mechanizmy nawoływania do przemocy w sieci są ścigane nawet wtedy, gdy komentujący sam nikogo nie atakuje. Uczeń, który w komentarzach pod filmem zachęca innych do „pobicia rekordu" w ataku na szkołę (nawoływanie do zbrodni – do 3 lat więzienia) albo publicznie gloryfikuje i chwali sprawców ataków w Ostrołęce czy Leszczydole-Nowinach (pochwalanie przestępstwa – do roku pozbawienia wolności), popełnia przestępstwo z urzędu.

4. **Przygotowanie do zabójstwa (art. 148 § 5 Kodeksu karnego):** Jeżeli za wpisami w sieci idą realne czynności – gromadzenie niebezpiecznych przedmiotów, tworzenie planu ataku, mapy szkoły czy wyszukiwanie instrukcji konstruowania ładunków – sprawa przestaje

dotyczyć fałszywego alarmu. Za samo przygotowanie do zbrodni zabójstwa grozi **od 2 do 15 lat pozbawienia wolności**.

## „Przecież jestem nieletni!" – jak w rzeczywistości wygląda odpowiedzialność ze względu na wiek?

Wielu uczniów żyje w błędnym przekonaniu, że do ukończenia 18. roku życia są prawnie nietykalni. Warto znać dokładne progi wiekowe wynikające z **Kodeksu karnego** oraz **Ustawy o wspieraniu i resocjalizacji nieletnich**, aby móc rzeczowo uświadomić klasę:

| **Wiek ucznia** | **Jak traktuje go polskie prawo?** | **Jakie konsekwencje może ponieść?** |
|---|---|---|
| **10–18 lat (w szczególności poniżej 13. r.ż.)** | Postępowanie w sprawach o **demoralizację** przed Sądem Rodzinnym (może dotyczyć każdego nieletniego od 10. do 18. roku życia). | Upomnienie, nadzór kuratora sądowego, zobowiązanie do określonego zachowania (np. przeproszenia nauczyciela), zobowiązanie rodziców do ścisłej współpracy ze szkołą i poradnią. |
| **13–17 lat** | Odpowiedzialność za **czyn karalny** przed Sądem Rodzinnym. *(Uwaga: po ukończeniu **15 lat** – a w skrajnych przypadkach zabójstwa nawet **14 lat** – przy najcięższych zbrodniach, np. zabójstwie lub ciężkim uszczerbku na zdrowiu, nieletni może odpowiadać przed sądem jak dorosły!)* | Nadzór kuratora, prace społeczne, przepadek przedmiotów (np. zatrzymanie telefonu użytego do przestępstwa), umieszczenie w młodzieżowym ośrodku wychowawczym (MOW), okręgowym ośrodku wychowawczym, a w najpoważniejszych sprawach – w **zakładzie poprawczym**. |
| **Od 17 lat** | **Pełna odpowiedzialność karna jak osoba dorosła!** | 17-letni uczeń klasy III lub IV liceum czy technikum w świetle prawa karnego **jest już dorosły**. Staje przed zwykłym sądem karnym, grozi mu grzywna, wyrok w zawieszeniu, wpis do Krajowego Rejestru Karnego (brudna karta karna zamykająca drogę do wielu zawodów), a nawet bezwzględne więzienie. |

Co istotne, niezależnie od wieku ucznia, za szkody majątkowe lub krzywdę wyrządzoną nauczycielowi (np. zniszczony sprzęt, porysowane auto, zadośćuczynienie za naruszenie dóbr osobistych w sieci) na gruncie prawa cywilnego (art. 426 i 427 Kodeksu cywilnego) bardzo często **odpowiadają finansowo rodzice** z tytułu braku należytego nadzoru.

## Gdzie kończą się uprawnienia nauczyciela, a kiedy działa obrona konieczna?

Znajomość prawa to także wiedza o tym, gdzie przebiega granica uprawnień pedagoga, aby w sytuacji kryzysowej nie narazić się na zarzut przekroczenia kompetencji:

1. **Zakaz osobistego przeszukiwania uczniów:** Nauczyciel nie jest funkcjonariuszem Policji – w standardowych warunkach nie ma prawa siłą opróżniać kieszeni ucznia ani przeszukiwać jego plecaka. Jeżeli zachodzi podejrzenie, że uczeń posiada niebezpieczny przedmiot (np. nóż) lub nielegalne substancje, należy zażądać dobrowolnego okazania zawartości torby w obecności dyrektora (lub innego pracownika szkoły), odizolować potencjalne zagrożenie i natychmiast wezwać Policję.

2. **Prawo do obrony koniecznej (art. 25 Kodeksu karnego) i stanu wyższej konieczności (art. 26 Kodeksu karnego):** Powyższe ograniczenia ustępują w momencie bezpośredniego, bezprawnego zamachu na życie lub zdrowie! Jeżeli w szkole dochodzi do fizycznego ataku (np. uczeń wyciąga niebezpieczne narzędzie lub rzuca się z pięściami na innego ucznia bądź pracownika szkoły), nauczyciel ma **pełne, ustawowe prawo do obrony koniecznej** – włącznie z fizycznym obezwładnieniem napastnika, odebraniem mu przedmiotu i użyciem środków współmiernych do odparcia ataku, aby ratować życie i zdrowie własne oraz podopiecznych.

3. **Jak nie obrócić prawa przeciwko sobie w świecie cyfrowym?** Nawet najlepsza tarcza prawna nie zadziała, jeśli nauczyciel sam zignoruje procedury bezpieczeństwa opisane w poprzednich rozdziałach. Używanie prywatnego Messengera do omawiania problemów uczniów, wysyłanie zbiorczych maili do rodziców z jawnymi adresami w polu „DW" zamiast „UDW", pożyczanie swojego hasła do e-dziennika na czas zastępstwa, zostawienie otwartego dziennika na komputerze podczas przerwy czy wklejanie niezanonimizowanych orzeczeń z poradni do darmowych czatbotów AI to działania, które z pokrzywdzonego mogą uczynić osobę winną naruszenia przepisów RODO. Z kolei prowadzenie komunikacji wyłącznie przez e-dziennik (np. Librus) daje nauczycielowi oficjalną, niepodważalną dokumentację, która chroni go w razie jakichkolwiek sporów z rodzicami lub dyrekcją.

## Co zrobić krok po kroku, gdy padniesz ofiarą ataku w sieci lub w szkole?

Gdy dojdzie do incydentu – niezależnie od tego, czy są to groźby, wygenerowany Deepfake, fałszywe konto czy znieważenie – o skuteczności prawa decydują pierwsze godziny i prawidłowe zabezpieczenie śladów:

1. **Zabezpiecz dowody cyfrowe (sam zrzut ekranu to za mało!):** Sam screen z telefonu łatwo podważyć przed sądem jako grafikę możliwą do przerobienia w kilka minut. Zawsze

skopiuj i zapisz **pełny adres URL** profilu sprawcy oraz konkretnego wpisu/filmu, zanotuj dokładną datę i godzinę publikacji, pobierz oryginalny plik wideo, a w przypadku wiadomości e-mail – zachowaj jej pełny nagłówek techniczny. Pokaż materiał na żywo (na ekranie urządzenia) innemu nauczycielowi lub dyrektorowi, aby zyskać naocznego świadka.

2. **Sporządź oficjalną notatkę służbową:** Opisz dokładnie i bez emocji przebieg zdarzenia, wskaż datę, godzinę, świadków oraz załącz zabezpieczone materiały.

3. **Złóż pisemne zgłoszenie do dyrektora szkoły:** Powołaj się na **art. 63 ust. 2 Karty Nauczyciela**, przypominając, że dyrektor oraz organ prowadzący mają obowiązek wystąpić w Twojej obronie z urzędu.

4. **Powiadom organy ścigania i instytucje zewnętrzne:** W przypadku gróźb, napaści, fałszywych alarmów, kradzieży tożsamości czy znieważenia zawiadom Policję (w sprawach internetowych warto wskazać Centralne Biuro Zwalczania Cyberprzestępczości). Nielegalne treści i incydenty w sieci zgłoś również do **CERT Polska** (incydent.cert.pl) lub **Dyżurnet.pl**, a jeśli wyciekły Twoje dane osobowe lub hasła – poinformuj szkolnego Inspektora Ochrony Danych (IOD) i zastrzeż numer PESEL w aplikacji mObywatel.