

Bezpieczny i odpowiedzialny w sieci





5 h 36 min w dni powszednie

Badania wskazują, że młodzi ludzie spędzają coraz więcej czasu online. Badania „Nastolatki 3.0” wykazało, że jest to średnio 5 godzin i 36 minut dziennie

Źródło: Raport „Nastolatki 3.0” – Państwowy Instytut Badawczy NASK



6 h 16 min w weekend

... oraz 6 godzin i 16 minut w weekendy.
To ponad 25 % doby!

Źródło: Raport „Nastolatki 3.0” – Państwowy Instytut Badawczy NASK

Cele naszego spotkania:

-  Nauczysz się rozpoznawać **manipulację i fake newsy**.
-  Dowiesz się, jak skutecznie **chronić swoje dane** i konta w Internecie.
-  Poznasz możliwości i zagrożenia związane ze sztuczną inteligencją oraz nauczysz się rozpoznawać treści generowane przez AI.
-  Zrozumiesz, jak reagować na **hejt, cyberprzemoc** i inne zagrożenia w sieci.
-  Będziesz korzystać z mediów społecznościowych w sposób świadomy, bezpieczny i odpowiedzialny.
-  Rozwiniesz krytyczne myślenie oraz umiejętność weryfikowania informacji, dzięki czemu staniesz się bardziej świadomym użytkownikiem Internetu i aktywnym uczestnikiem życia społecznego.

Agenda

1. AI – supermoc czy zagrożenie? 🤖
2. Nie daj się złapać! Jak działają cyberprzestępcy? 🕵️
3. Prawda czy fake? Walka z dezinformacją 🔍
4. Słowa mają moc – hejt i cyberprzemoc 💬
5. Twoje dane, Twoja sprawa 🔒
6. Internet bezpieczniejszy dzięki Tobie 🛡️
7. Zostań świadomym graczem w cyfrowym świecie 🌐

**Bez czego trudniej byłoby Wam
wytrzymać jeden dzień –
telefonu czy Internetu?**

Szanse



- 🎓 **Uczysz się szybciej** – kursy online, YouTube, ChatGPT, materiały do matury, języki obce.
- 🌐 **Poznajesz świat** – kontakt z ludźmi z innych krajów, nowe kultury, wydarzenia na żywo.
- 💬 **Utrzymujesz kontakt** – rodzina, znajomi, wspólne projekty, komunikatory.
- 🎨 **Rozwijasz pasje** – fotografia, muzyka, sport, programowanie, grafika, tworzenie filmów.
- 🚀 **Budujesz swoją przyszłość** – uczysz się nowych umiejętności, tworzysz portfolio
- 🤖 **Korzystasz z AI** – szybciej się uczysz, tworzysz prezentacje, rozwiązujesz problemy.

Zagrożenia



- 🗞️ **Fake news i manipulacja** – nie każda informacja w sieci jest prawdziwa. Łatwo paść ofiarą dezinformacji.
- 👤 **Utrata prywatności** – zdjęcia, lokalizacja czy dane osobowe mogą trafić w niepowołane ręce.
- 💣 **Hejt i cyberprzemoc** – obraźliwe komentarze, wyśmiewanie czy nękanie mogą mieć realne konsekwencje.
- 🕸️ **Oszustwa internetowe** – phishing, fałszywe sklepy, wyłudzenie pieniędzy i przejmowanie kont.
- 📱 **Uzależnienie od ekranu** – godziny spędzone na scrollowaniu mogą zabierać czas, energię i pogarszać koncentrację.
- 🎬 **Deepfake i treści AI** – coraz trudniej odróżnić prawdę od materiałów wygenerowanych przez sztuczną inteligencję.

Internet to **potężne narzędzie**. Może pomóc Ci się **rozwijać** albo stać się źródłem **problemów**.

O tym, po której stronie będziesz, decydują przede wszystkim **Twoje wybory** i umiejętność krytycznego myślenia



Cyberbezpieczeństwo to sposób
ochrony naszych urządzeń, kont,
danych i pieniędzy przed
osobami, które chcą je ukraść,
wykorzystać lub zniszczyć.

Twoje konto zostało zablokowane.
Kliknij **tutaj**, aby je odblokować

„...dopłać 2 zł do przesyłki”

Hej! Popatrz na tego tiktoka!

Siemka! Podeszlesz mi kod blisk, zablokowałem przypadkowo konto



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.

Te pytania możemy zastąpić jednym...

„Hej! Czy podeślesz mi swoje wszystkie dane osobiste, numery konta bankowego, hasło do niego, numery karty kredytowej, pin... i **w sumie to najlepiej wszystkie swoje pieniądze?**”

Zapamiętaj!

**Największą luką w cyberbezpieczeństwie
najczęściej nie jest komputer... tylko
człowiek.**

Jak działają cyberprzestępcy?

Zaczynają od emocji, nie od technologii



Wykorzystują:

- Pośpiech
- Strach
- Ciekawość
- Chęć pomocy
- **Obietnicę łatwego zysku!**

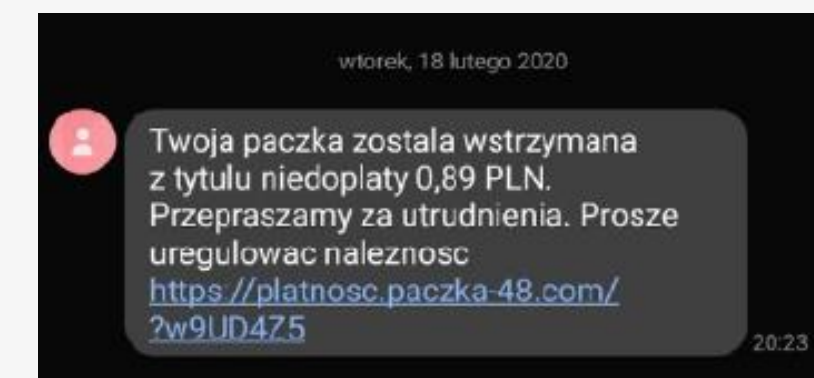
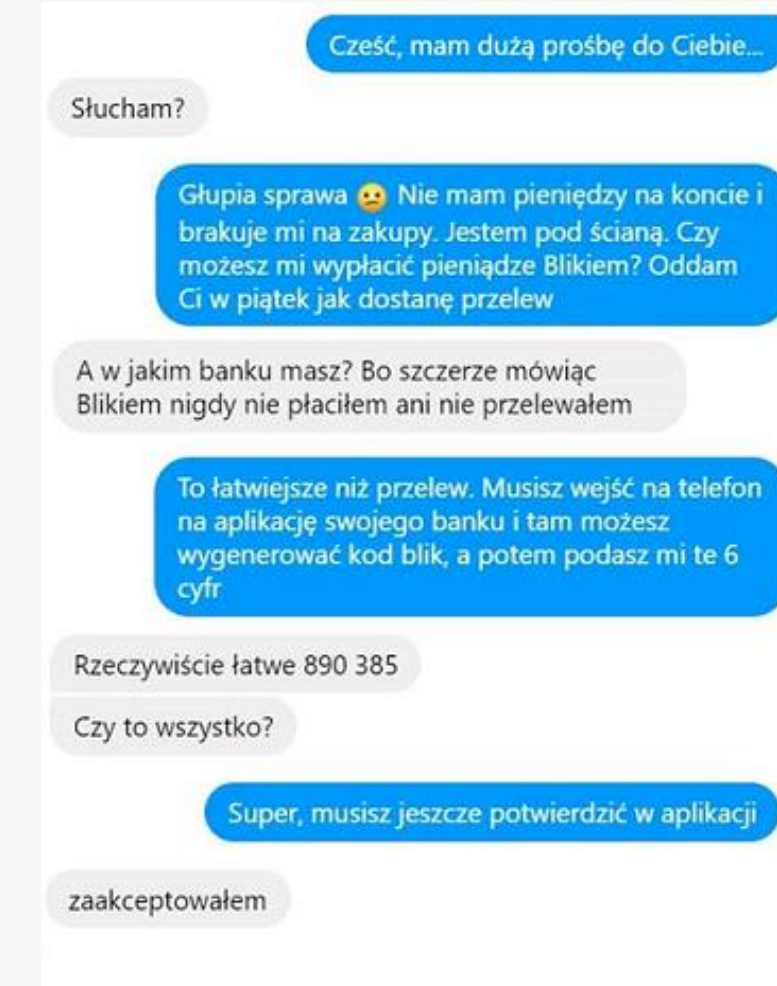
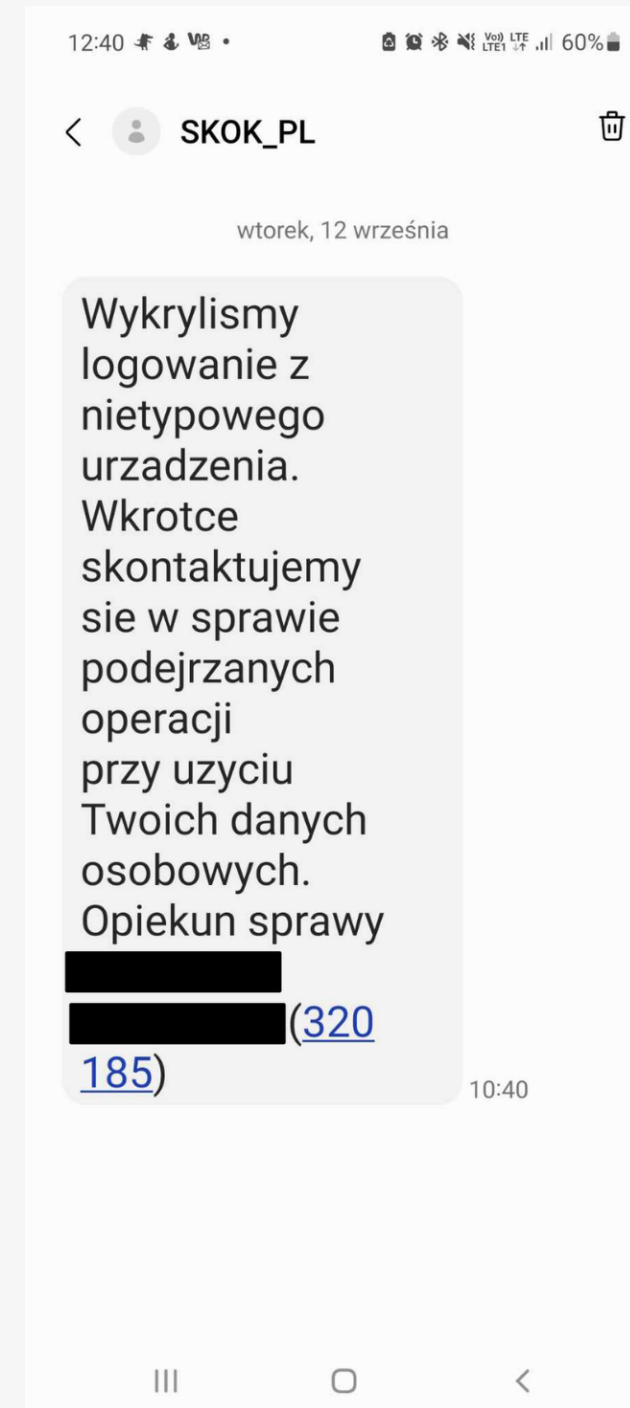
Socjotechnika

To manipulowanie człowiekiem w taki sposób, aby sam przekazał swoje dane lub wykonał działanie, którego normalnie by nie zrobił.

"Masz tylko 10 minut, żeby odzyskać konto!,"

„Dopłać za przesyłkę teraz!”

„Pożyczysz mi stówkę? Jestem z Dianą w McDonaldzie i będzie wstyd jak nie zapłacę”



Jak rozpoznać fake newsy i manipulację?



1. 🔥 Zwróć uwagę na emocje

Fake newsy często mają wywołać:

- strach,
- złość,
- szok,
- sensację.

2. 📄 Sprawdź źródło informacji

Zanim uwierzysz:

kto opublikował tę informację?

czy jest to znane i wiarygodne źródło?

czy autor podaje swoje źródła?

Brak autora lub anonimowy profil = sygnał ostrzegawczy.

3. 🔍 Nie ufaj samemu nagłóvkowi

Nagłówki często są tworzone tak, aby zdobyć kliknięcia.

Przykład:

„SZOK! Naukowcy ukrywali to przez lata!”

Sprawdź całą treść – nie tylko pierwsze zdanie.



4. 📖 Sprawdź informację w kilku miejscach

Jedna publikacja to za mało.

Poszukaj:

- oficjalnych komunikatów,
- innych niezależnych źródeł,
- potwierdzenia przez ekspertów.

5. ⌚ Nie działaj pod presją czasu

Manipulacja często wygląda tak:

❌ „Masz tylko 5 minut!”

❌ „Udostępnij zanim usuną!”

❌ „Nikt nie chce, żebyś o tym wiedział!”

Pośpiech ogranicza krytyczne myślenie.

6. 🧠 Zastanów się: „Czy chcę w to wierzyć?”

Czasami łatwiej wierzymy informacjom, które:

potwierdzają nasze poglądy,
pasują do naszych emocji,
pokazują "ukrytą prawdę".

Jak rozpoznać fake newsy i manipulację?

Zasada STOP przed udostępnieniem

S – Sprawdź źródło

T – Tylko nie działaj impulsywnie

O – Oceń wiarygodność

P – Podaj dalej dopiero, gdy masz pewność

Największą bronią przeciwko dezinformacji nie jest technologia – jest nią krytyczne myślenie.



Zagrożenia związane ze sztuczną inteligencją

-  1. Deepfake – fałszywe filmy i nagrania (film o najbliższych, nagranie głosu z prośbą o przelew)
-  2. Fałszywe zdjęcia (szerzenie fake newsów, wzbudzanie emocji, oszustwa)
-  3. Bardziej przekonujące oszustwa (e-mail od banku, wiadomość od kuriera, SMS ze szkoły, wiadomość od znajomego)
-  4. Manipulacja w mediach społecznościowych (boty i ich komentarze, profile obcych osób, odpowiedzi ...)
-  5. Naruszenie prywatności (wykorzystanie Twojego hasła, wykorzystanie dokumentów przesłanych do agenta, **wykorzystanie danych osobowych**)



Jak korzystać z AI odpowiedzialnie?

-  Traktuj AI jako pomoc, a nie nieomyłne źródło wiedzy.
-  Weryfikuj informacje w wiarygodnych źródłach.
-  Nie udostępniaj poufnych danych.
-  Zwracaj uwagę na materiały mogące być wygenerowane przez AI.
-  Korzystaj z AI zgodnie z zasadami etyki i prawa.

Hejt i cyberprzemoc





Co 3 osoba

...doświadcza obecnie przemocy online.

Źródło: Raport „Nastolatki” – Państwowy Instytut Badawczy NASK



Okej ... a czym w ogóle jest cyberprzemoc? Czy byłeś jej świadkiem?

Cyberprzemoc (cyberbullying, agresja elektroniczna, elektroniczna przemoc rówieśnicza) to przemoc wyrządzana za pomocą narzędzi elektronicznych: **telefonu, komunikatorów, mediów społecznościowych, gier online czy poczty e-mail**. Od zwykłego konfliktu odróżniają ją trzy cechy: jest **intencjonalna** (sprawca chce skrzywdzić), **powtarzalna** (to seria zachowań, nie pojedynczy incydent) i oparta na **nierównowadze** sił (ofiara nie może się skutecznie bronić).

Choć może dotknąć każdego, najczęściej dotyka dzieci i młodzież.

Rodzaje przemocy i jej formy

- **hejt** – obraźliwe i dyskredytujące komentarze publikowane w internecie
- **cyberstalking** – uporczywe nękanie wiadomościami, telefonami i śledzenie aktywności ofiary,
- **publikowanie materiałów ośmieszających** – zdjęć, filmów i memów wymierzonych w konkretną osobę,
- **doxing** – gromadzenie i publikowanie prywatnych danych ofiary,
- **włamania** – na pocztę elektroniczną lub konta w mediach społecznościowych,
- **podsywanie się** – zakładanie fałszywych profili z użyciem cudzego imienia i wizerunku,
- **wykluczanie** – celowe usuwanie lub pomijanie osoby w grupach i społecznościach internetowych,
- **sexting bez zgody i sextortion** – rozsyłanie intymnych materiałów oraz wyłudzenie ich, a następnie szantażowanie ofiary ich publikacją,
- **flood** – zalewanie skrzynki lub czatu masą wiadomości,
- **szantaż** – groźba ujawnienia kompromitujących materiałów.



Ale również!

- **Shareparenting** (publikowanie przez rodziców zdjęć, informacji o dziecku, jego wizerunku)
- **Patostreamy** (transmisje na żywo pokazujące przemoc, libacje)
- Challenge (niebezpieczne wyzwania kierowane przez „Internet”)

Jakie są przyczyny cyberprzemocy? Co kieruje takimi ludźmi?

- **Względna anonimowość** (za Nickiem, awatarem, fejkową nazwą łatwo się ukrywać)
- **Efekt tłumu, rozhamowania** - ekran znosi naturalne hamulce, sprawca nie widzi łez ani strachu ofiary, więc nie dostaje sygnałów, które w bezpośrednim kontakcie powstrzymałyby agresję.
- **Publiczność** - Upokorzenie w sieci ma świadków liczonych w setkach, a bierność obserwatorów (lajki, udostępnienia, brak reakcji) wzmacnia sprawcę.
- **Nuda i potrzeba statusu społecznego** - część sprawców traktuje dręczenie jako rozrywkę lub sposób na zbudowanie pozycji w grupie rówieśniczej.
- **Przenoszenie konfliktów ze świata offline**



Gdzie szukać pomocy?



Telefon zaufania dla dzieci i młodzieży Fundacji Dajemy Dzieciom Siłę:

116 111

oraz

Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka: **800 12 12 12**.

Oba działają całą dobę, 7 dni w tygodniu, połączenia są bezpłatne, a rozmowa anonimowa.

W sytuacji bezpośredniego zagrożenia życia dzwoń pod **112**.



**Pomóż koledze/koleżance, gdy
dzieje mu/jej się krzywda.**

Analiza sytuacji

Kuba wrzucił zdjęcie koleżanki z klasowej wycieczki. Ktoś je przerobił. W ciągu jednego wieczoru zdjęcie zostało udostępnione ponad 300 razy.

W komentarzach pojawiły się wyzwiska i obraźliwe żarty. Część osób nic nie napisała, ale udostępniła post dalej.

- Czy to był tylko żart?
- Kto ponosi odpowiedzialność?
- Czy osoby, które tylko udostępniły post, również mają wpływ na sytuację?
- Jak można było zareagować?
- Co Ty zrobiłbyś na miejscu świadka?

• Czy chciałbyś być na miejscu koleżanki?

Jak reagować na cyberprzemoc?

- Nie odpowiadaj agresorowi,
- Zabezpiecz dowody,
- Zablokuj sprawcę i zgłoś treści na platformie,
- Powiedz zaufanemu dorosłemu, wychowawcy, pedagogowi,
- Jeśli sytuacja jest poważna – zgłoś to służbom!

Cyberprzemoc nie kończy się sama. Im szybciej zareagujesz, tym większa szansa na zatrzymanie sprawcy i ochronę siebie lub innych.

Czy masz zainstalowaną tę aplikację?

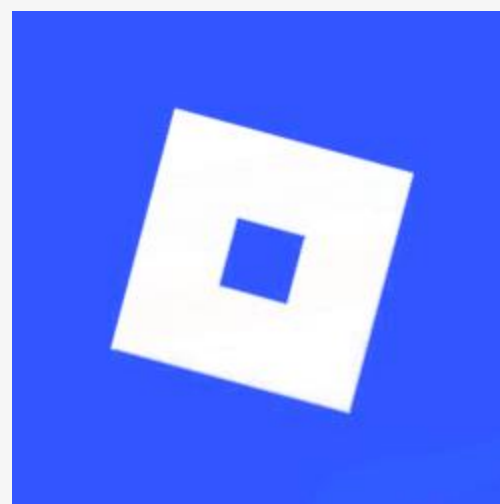














Co łączy te aplikacje?

Imię i nazwisko

Adres zamieszkania

Mój wizerunek

Podana nazwa szkoły

Moje koleżanki

Adres e-mail

Numer telefonu

Miejsce pobytu

Publiczne życie

Wykorzystywanie
waszej galerii zdjęć

Udostępniona lokalizacja



Co zaliczamy do danych osobowych?

-  imię i nazwisko,
-  data urodzenia,
-  adres zamieszkania,
-  numer telefonu,
-  adres e-mail,
-  wizerunek,
-  lokalizacja,
-  nazwa szkoły,
-  numer PESEL lub dokumentu,
-  dane płatnicze.



Dlaczego ktoś chce je zdobyć?

Przestępcy mogą wykorzystać je do:

- kradzieży kont,
- podszywania się pod Ciebie,
- wyłudzenia pieniędzy,
- oszustw finansowych,
- szantażu.

Najczęstsze błędy młodych użytkowników



Udostępnianie zbyt wielu informacji

Przykłady:

- zdjęcie legitymacji szkolnej,
- karta pokładowa,
- bilet na koncert,
- dokumenty,
- zdjęcie nowej karty bankowej.

Włączona lokalizacja

Publikując relacje pokazujesz:

- gdzie mieszkasz,
- gdzie chodzisz do szkoły,
- kiedy nie ma Cię w domu,
- gdzie obecnie się znajdujesz.



Publiczne profile

Zastanów się:

- Czy każdy musi widzieć Twoje zdjęcia?
- Czy każdy powinien znać Twoją szkołę?
- Czy każdy powinien widzieć Twoją lokalizację?

Zdjęcia innych osób

Czy ta osoba zgodziła się na publikację?

Przed udostępnieniem zadaj sobie pytanie

**Czy podałbym te informacje
przypadkowej osobie na
ulicy?**

Dobre praktyki bezpiecznego mnie w Internecie

Aktualizuj swoje urządzenia

Aktualizuj system, aplikacje i programy.



Używaj silnych haseł

(Kuba123, Oliwia1, Jola01032010)

Nie klikaj podejrzanych linków

"Kliknięcie trwa sekundę, konsekwencje mogą trwać znacznie dłużej."

Sprawdzaj źródła informacji

Nie wszystko, co widzisz w internecie, jest prawdą.

Szanuj innych

Internet nie zwalnia z kultury osobistej.



Chroń swoje dane

adres, numer telefonu, dokumenty, lokalizacja, prywatne zdjęcia.

Zgłaszaj nadużycia

Nie ignoruj: hejtu, cyberprzemocy, fałszywych kont, oszustw.

Myśl przed publikacją

Czy chciałbym, żeby zobaczyli to rodzice, nauczyciele lub przyszły pracodawca?

Korzystaj świadomie z AI

AI może pomagać, ale nie zawsze ma rację.

 weryfikacja

 AI

 hasło

 dane

Ja w sieci

 kultura

 aktualizacje

 zgłoszenia

 linki

 <https://haveibeenpwned.com/>

 *Największym
zabezpieczeniem w sieci jesteś
Ty
Twoja wiedza, ostrożność
i świadome decyzje.*



Internet jest narzędziem

*to od nas zależy, czy
wykorzystamy go do rozwoju,
czy narazimy się na zagrożenia.*



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.



*Cyberprzestępcy często
nie atakują technologii*

*wykorzystują ludzkie
emocje i nieuwagę*



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.



***Jedno słabe hasło
może otworzyć drzwi
do całego cyfrowego
życia.***



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.

 *Nie każda informacja,
którą widzisz, zasługuje na
udostępnienie*

***najpierw sprawdź, potem
uwierz.***



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.

 *To, co publikujesz
w Internecie zostaje tam
na zawsze

chroń swoją prywatność.*



*Po drugiej stronie ekranu
zawsze jest **człowiek***

*słowa online mają realne
konsekwencje.*



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



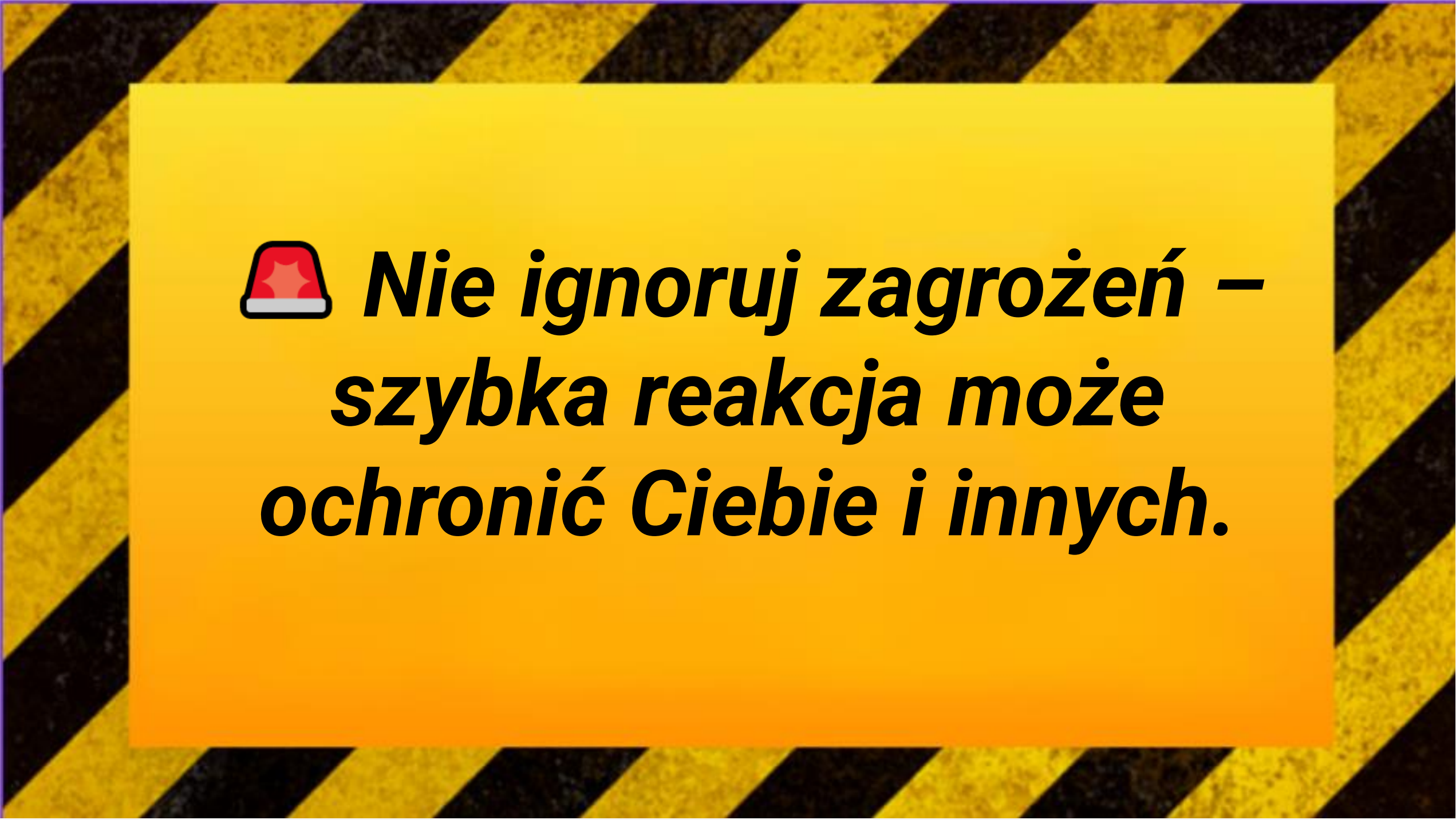
ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.



*Twoje zachowanie online
buduje Twój cyfrowy ślad
i wpływa na innych.*



 ***Nie ignoruj zagrożeń –
szybka reakcja może
ochronić Ciebie i innych.***

Myśl. Sprawdzaj.
Chroń siebie i innych.
Bezpieczeństwo w sieci
zaczyna się od Ciebie.

QUIZ



Pytanie 1

Otrzymujesz SMS:

„Twoja paczka została zatrzymana. Dopłać 1,99 zł, aby ją odebrać. Kliknij link.”

Co robisz?

- A) Klikam – to tylko 1,99 zł
- B) Przekazuję SMS znajomym, żeby ich ostrzec
- C) Sprawdzam przesyłkę w oficjalnej aplikacji przewoźnika i nie klikam linku
- D) Podaję dane karty, żeby szybko zapłacić



Pytanie 2

Które hasło jest najbezpieczniejsze?

- A) Kuba123
- B) 01012010
- C) MojeHaslo
- D) Rower!Las7Kawa#2026



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.

QUIZ



Pytanie 3

Znajomy pisze:

„Hej, pilnie potrzebuję pieniędzy. Podeślij mi kod BLIK.”

Co robisz?

- A) Wysyłam kod, bo to ziomeczek
- B) Najpierw dzwonię i potwierdzam sytuację
- C) Wysyłam połowę kwoty
- D) Publikuję jego wiadomość w Internecie, żeby ostrzec innych



Pytanie 4

Która sytuacja może być cyberprzemocą?

- A) Konstruktywna krytyka filmu
- B) Prywatna rozmowa ze znajomym
- C) Publikowanie obraźliwych komentarzy i wyśmiewanie osoby
- D) Udostępnienie oficjalnego artykułu



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.

QUIZ



Pytanie 5

Czy zdjęcie w internecie zawsze przedstawia prawdziwą sytuację?

- A) Tak, zdjęcia zawsze pokazują prawdę
- B) Nie, zdjęcia mogą być przerobione lub wygenerowane przez AI
- C) Tak, jeśli wygląda realistycznie
- D) Tylko zdjęcia celebrytów mogą być fałszywe



Pytanie 6

Która informacja NIE powinna być publicznie udostępniana?

- A) Ulubiony film
- B) Hobby
- C) Zdjęcie dokumentu z widocznymi danymi
- D) Opinia o książce

QUIZ



Pytanie 7

Otrzymujesz obraźliwe wiadomości w internecie. Co robisz?

- A) Odpowiadam jeszcze bardziej agresywnie
- B) Usuwaam wszystko i nikomu nie mówię
- C) Zachowuję dowody, blokuję sprawcę i zgłaszam problem
- D) Udostępniam wiadomości publicznie



Pytanie 8

Wymień jakie Twoje dane są wrażliwe....



Ministerstwo
Edukacji Narodowej



Minister
Edukacji



ŚWIADOMI W SIECI
AKTYWNI W SPOŁECZEŃSTWIE

Vd
FUNDACJA VOX DOCET

Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach programu
„Kompas Młodego Obywatela”.

DZIĘKUJEMY że jesteś z nami

„Projekt dofinansowany ze środków budżetu państwa,
przyznanych przez Ministra Edukacji w ramach
programu „Kompas Młodego Obywatela”.

