

Bezpieczeństwo cyfrowe w lokalnej społeczności

– wnioski i rekomendacje po pierwszej
edycji Łowickiego Forum Bezpiecznego
Internetu





Od Autorki

Cyberbezpieczeństwo to dziś wspólne wyzwanie całych społeczności – zarówno w skali globalnej, jak i w lokalnych środowiskach, w których żyjemy i pracujemy.

Fundacja Łowickie Forum Bezpiecznego Internetu powstała w celu prowadzenia edukacji, tworzenia neutralnej przestrzeni do rozmów o zagrożeniach cyfrowych oraz współtworzenia i wdrażania lokalnych rozwiązań na rzecz cyberbezpieczeństwa.

9 października 2025 zainaugurowaliśmy pierwszą edycję Forum, które zgromadziło ponad 150 uczestników i stało się początkiem lokalnej tradycji edukacji, networkingu i profilaktyki zagrożeń cyfrowych.

Dziękuję wszystkim, którzy wzięli udział w Forum oraz wsparli je merytorycznie, finansowo czy organizacyjnie. Szczególnie dziękuję Burmistrzowi Miasta Łowicza Mariuszowi Siewierze oraz Katarzynie Skierskiej Pięcie - Sekretarz Urzędu Miejskiego za współpracę oraz silne wsparcie. Publikację, którą oddajemy w Państwa ręce, zawdzięczamy wspólnemu wysiłkowi i zaangażowaniu wielu osób.

Podsumowanie powstało w ramach Akcji Masz Głos przy merytorycznym wsparciu Pracowni Zrównoważonego Rozwoju.

Anna Kędziora-Zabost

Prezes Zarządu Fundacji Łowickie Forum Bezpiecznego Internetu

Spis treści

01

Kontekst globalny

Dlaczego bezpieczeństwo cyfrowe jest sprawą lokalną

03

Forum

Przebieg pierwszej edycji

05

Wnioski ogólne po Forum

Wypracowane podczas Forum i z raportów zewnętrznych

07

Dalsze kroki

Projekty i inicjatywy na rzecz cyberbezpieczeństwa społeczności lokalnej

02

Cyberbezpieczeństwo

W Polsce i w regionie

04

Bezpieczeństwo cyfrowe dla edukacji

Warsztat World Café

06

Edukacja

Fundament bezpieczeństwa lokalnej społeczności



01. Kontext globalny

Zagroženia globalne, skutki lokalne

Kontekst globalny i europejski cyberbezpieczeństwa

- ❏ Cyberbezpieczeństwo to problem, który nie zna granic. W dzisiejszym świecie, gdzie miliardy ludzi są online, każdy z nas staje się potencjalnym celem cyberataku. Zrozumienie skali i natury tych globalnych zagrożeń jest kluczowe dla budowania skutecznych strategii obronnych na poziomie lokalnym.



Globalny zasięg

5,3 miliarda ludzi online w 2025 roku - co czyni każdego potencjalnym celem ataku cyfrowego.



Fale ransomware

Co 11 sekund na świecie dochodzi do ataku ransomware, paraliżującego firmy i instytucje.



Różnorodni agresorzy

Od państwowych aktorów, przez przestępców zorganizowanych, po hacktywistów – wszyscy stanowią poważne zagrożenie dla bezpieczeństwa online.

Kluczowe Globalne Zagrożenia Cybernetyczne

- ❏ W obliczu rosnącej digitalizacji, świat staje w obliczu coraz bardziej złożonych i zróżnicowanych zagrożeń cybernetycznych. Rozumienie ich charakteru jest pierwszym krokiem do skutecznej obrony lokalnej.



Ataki państwowe

Grupy wspierane przez różne siły polityczne prowadzą zaawansowane operacje szpiegowskie i sabotażowe. Ich celem jest destabilizacja infrastruktury krytycznej, kradzież danych strategicznych oraz wpływanie na politykę, co bezpośrednio zagraża suwerenności państw i bezpieczeństwu obywateli.



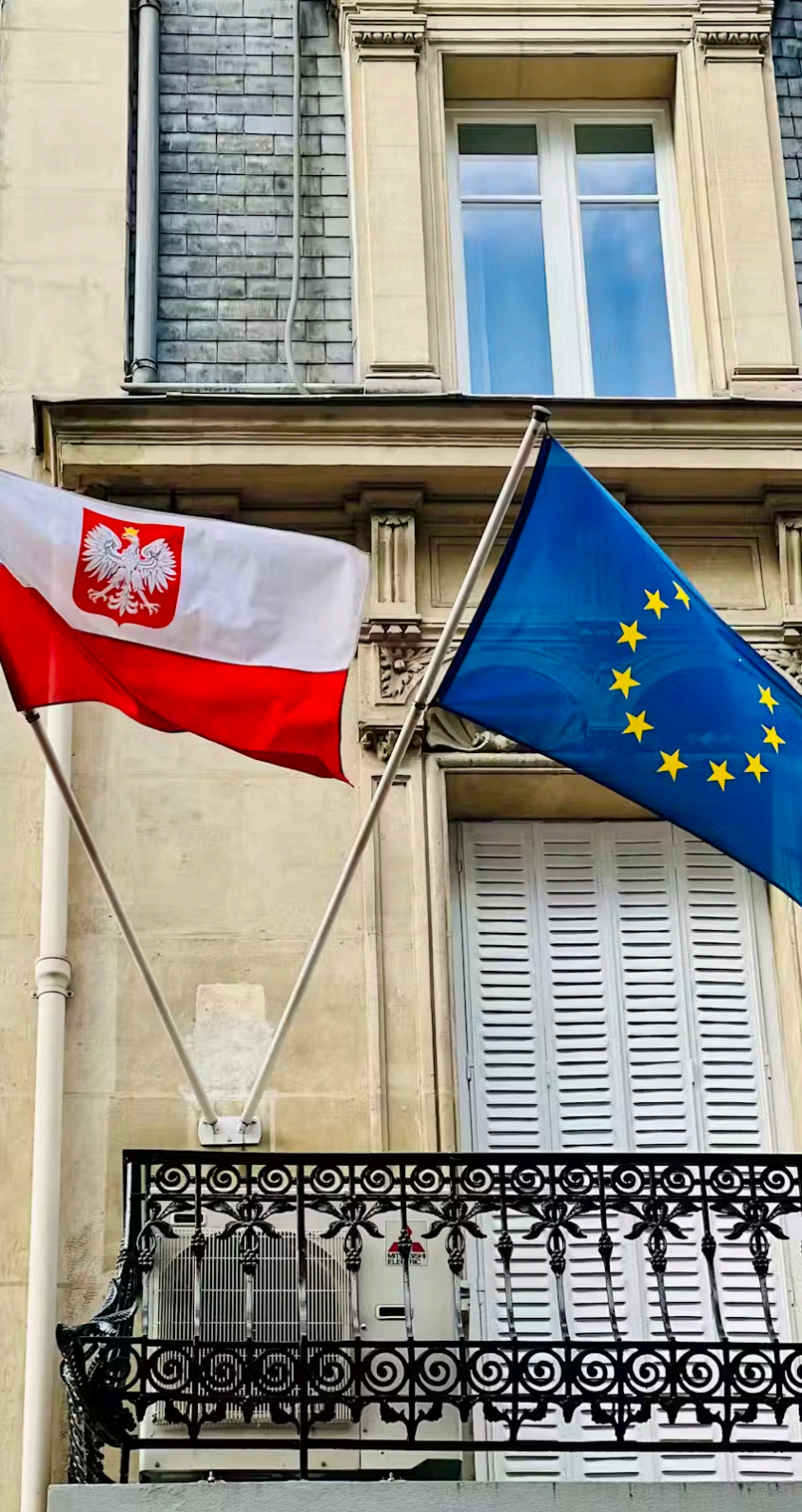
Przestępczość zorganizowana

Ransomware, kradzież tożsamości, oszustwa finansowe i wyłudzenia to główne narzędzia zorganizowanych grup przestępczych. Ich działania stają się coraz bardziej wyrafinowane, prowadząc do ogromnych strat finansowych dla firm i instytucji, a także poważnych konsekwencji dla indywidualnych ofiar.



Hacktywiści i terroryzm informacyjny

Motywowani ideologicznie lub politycznie, wykorzystują cyberataki do szerzenia dezinformacji, prowadzenia protestów cyfrowych i zakłócania działania kluczowych usług. Ich działania mogą prowadzić do paniki społecznej, utraty zaufania do instytucji i bezpośrednio wpływać na stabilność społeczną.



02.Cyberbezpieczeństwo

W Polsce i w regionie

Zagrożenia cyberbezpieczeństwa w Europie 2025

– Dane i Statystyki

Najszybciej rosnące zagrożenia w Europie (2025)



PHISHING I KRADZIEŻ TOŻSAMOŚCI

60% incydentów
inicjujących ataki

Źródło: Verizon Data Breach
Investigations Report 2025

Dodatkowa info: +80% udziału AI
w kampaniach phishingowych
(ENISA 2025)



DEZINFORMACJA I MANIPULACJA INFORMACJI

↑ **Rosnący trend** kampanii
FIMI (Foreign Information
Manipulation and
Interference)

Głównie: Aktorzy państwowi
i grupy hacktywistyczne

Źródło: ENISA 2025, European
External Action Service (EEAS)



CYBERPRZEMOC WOBEĆ DZIECI I MŁODZIEŻY

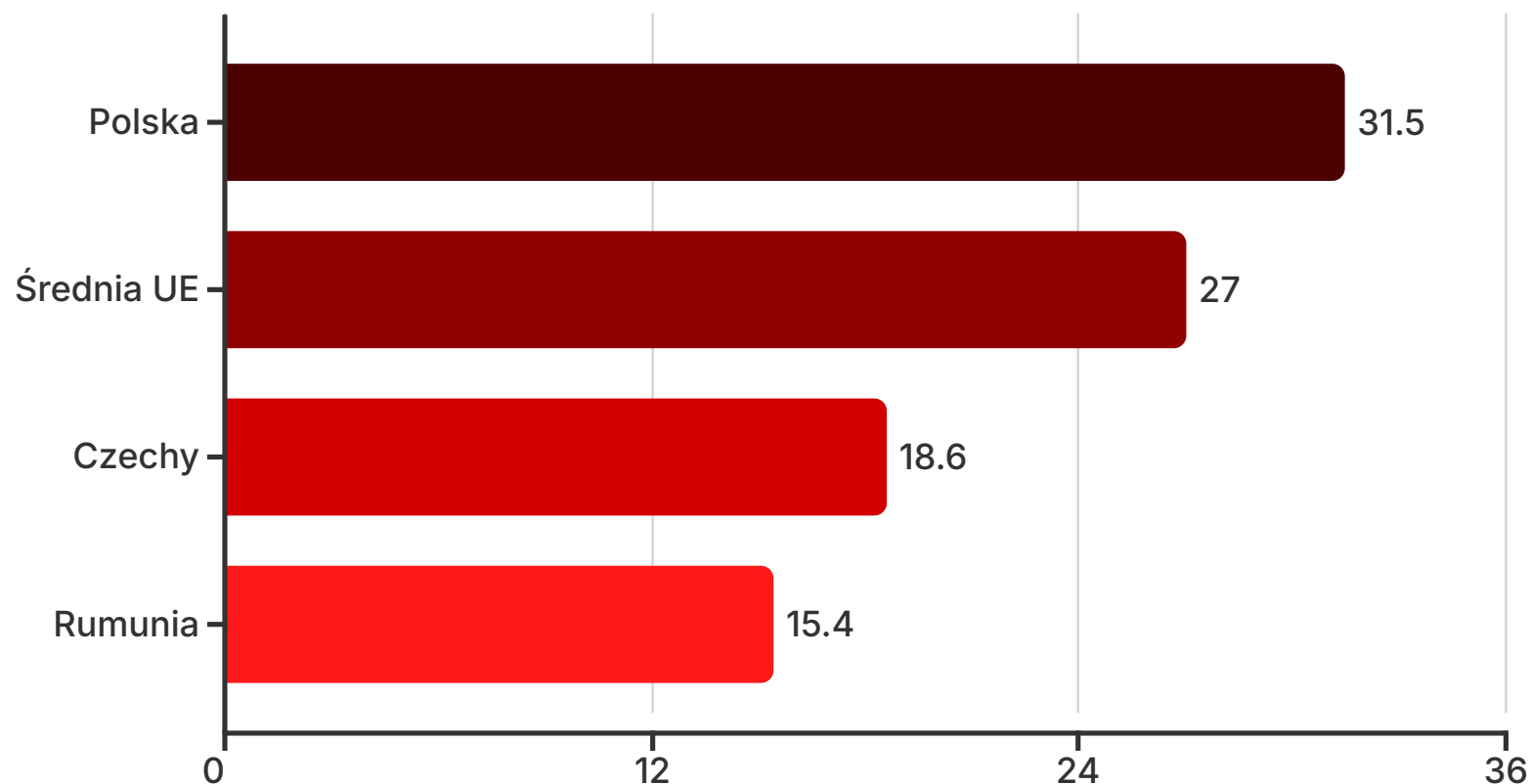
~15% (1 na 6) nastolatków
w Europie doświadczyło
cyberprzemocy

Znaczna część wyrażała obawy
przed hejtem i mową nienawiści

Źródło: WHO Europe Study 2024
(dane z 2022 r.)

Cyberprzemoc w UE – Polska liderem negatywnym

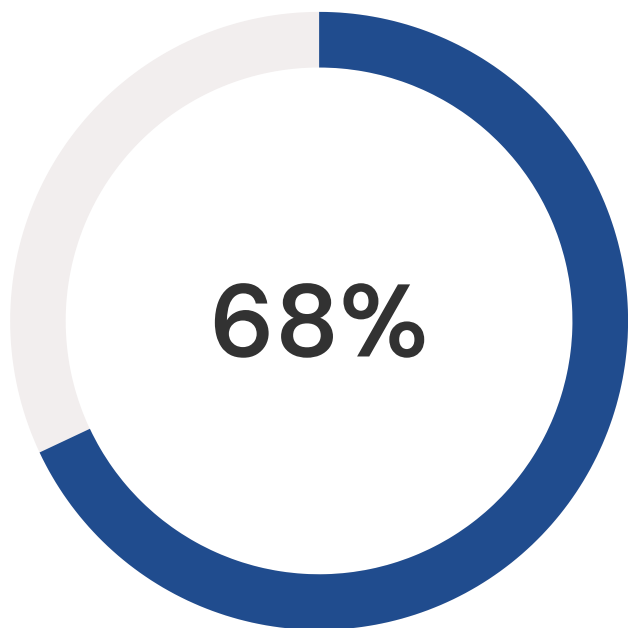
Polska odnotowała najwyższy odsetek młodych ludzi doświadczających cyberprzemocy w UE, znacznie przekraczając średnią europejską.



Źródło: Fundamental Rights Agency (FRA) – Survey 2019 | Dane reprezentacyjne UE | Implikacje: Polska wymaga priorytetowych działań

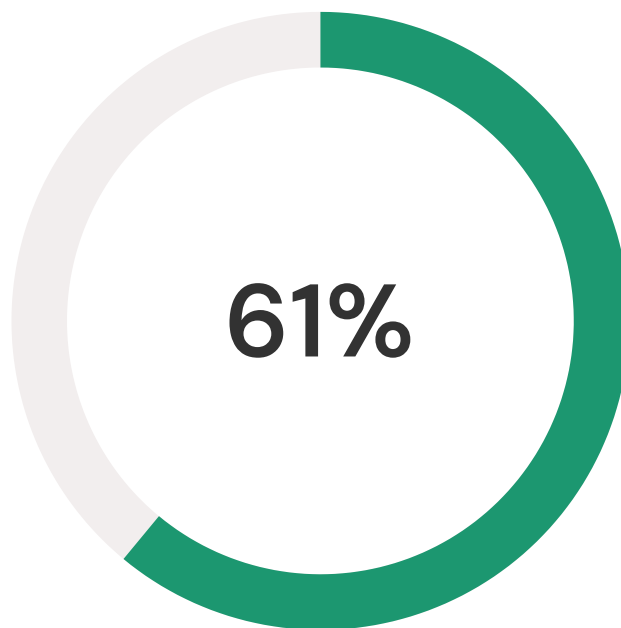
Największe zagrożenia cyfrowe w Polsce

Według danych Ministerstwa Cyfryzacji z 2025 roku, Polacy najbardziej obawiają się trzech rodzajów zagrożeń cyfrowych:



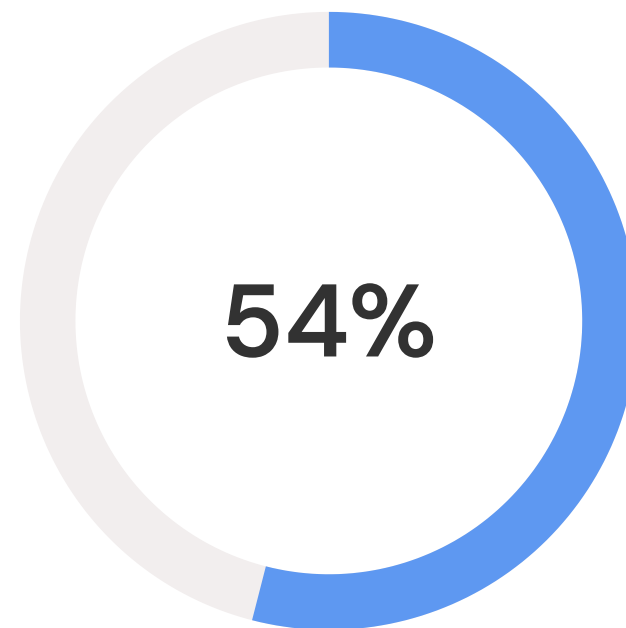
Phishing

Wyłudzenie danych osobowych i finansowych



Kradzież tożsamości

Przejęcie kont i profili w sieci



Dezinformacja

Fałszywe informacje oraz manipulacja

📌 Wzrost liczby zgłoszeń cyberincydentów o 62% w 2024 roku (dane NASK) pokazuje skalę problemu w Polsce.

Dzieci i młodzież w sieci

Raport "Internet Dzieci 2025"

Instytut Cyfrowego Obywatelstwa przeprowadził kompleksowe badanie dotyczące aktywności online najmłodszych użytkowników Internetu. Wyniki pokazują niepokojące trendy:

85%

Regularnie online

Dzieci w wieku 7-14 lat
korzysta z internetu
każdego dnia

4:29

Czas w sieci

Średni dzienny czas
spędzany przez dzieci
w Internecie (godz:min)

58%

Poniżej limitu wieku

Dzieci 7-12 lat ma konta
w social media mimo
wymogu 13+

1:55

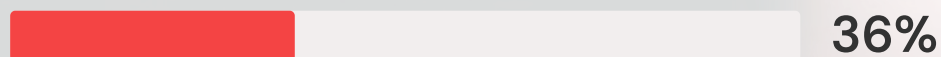
Oglądanie video

Średni dzienny czas
oglądania YouTube / TikTok
(godz:min)

Nastolatki w sieci

Raport "Nastolatki 2025" (NASK)

Badania przeprowadzone przez NASK wśród młodzieży w wieku 12-18 lat ujawniają głębokie problemy związane z bezpieczeństwem cyfrowym i zdrowiem psychicznym nastolatków.



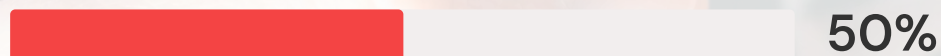
Problematyczne korzystanie z sieci

Blisko 36 % nastolatków wykazuje wysoki poziom uzależnienia od Internetu



Obawa przed hejtem

Młodych ludzi wskazuje hejt jako główne zagrożenie w sieci



Doświadczenie przemocy

Połowa nastolatków spotkała się z hejtem lub przemocą online



Gry online

Prawie 90% nastolatków gra w gry komputerowe przynajmniej raz w tygodniu



Hejt jest walutą. Jest narzędziem. Jest strategią. Dlaczego?
Bo wyzwala reakcję. Bo pozwala się wybić. Bo (co tu dużo mówić)
algorytm go uwielbia. Konflikt, kontrowersja, dramat. Wszystko,
co wywołuje emocje, podkreśla zasięg. A skoro hejt wzbudza
emocje, to znaczy, że działa.

Winni? My wszyscy. Bo konsumujemy go bez refleksji.
Bo lajkujemy. Bo podajemy dalej. Internet uczy nas, że nienawiść
to forma ekspresji. Że warto się „wyżyć”. Że można „pojechać”
komuś, bo się na czymś nie zna. Zwykle granice empatii
przesuwają się milimetr po milimetrze.

– Wojtek Kardyś, Ekspert w dziedzinie mediów społecznościowych
i digital marketingu. Keynote Speaker Łowickiego Forum
Bezpiecznego Internetu.

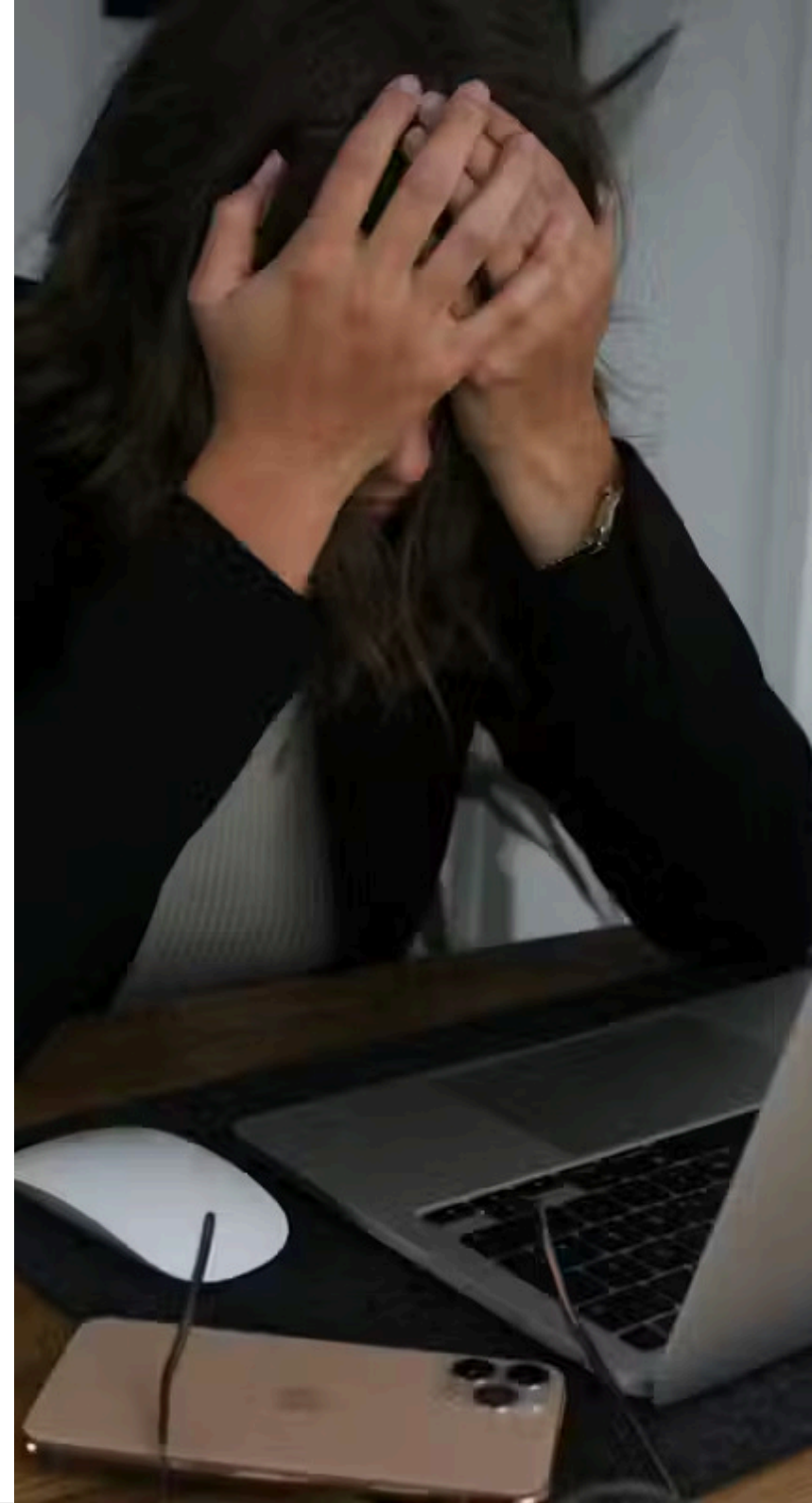
** Cytat pochodzi z najnowszej książki "HOMO DIGITALIS" Jak
Internet pożera nasze życie?*



84%

młodych ludzi najbardziej boi się hejtu

Jest to dla nich najważniejsze z zagrożeń – według najnowszych badań przeprowadzonych na zlecenie Rzeczniczki Praw Dziecka w lutym 2025 roku.



Dlaczego lokalne społeczności są kluczowe?

Choć zagrożenia mają charakter globalny, skuteczna ochrona cyfrowa budowana jest lokalnie.



Zaufanie i bliskość

Lokalne społeczności opierają się na bezpośrednich relacjach. Rodzice znają nauczycieli, nauczyciele znają samorządowców, wszyscy mieszkają w jednym mieście.



Szybkość reakcji

W małej społeczności można szybciej wypracować i wdrożyć skuteczne procedury reagowania na incydenty.



Dostosowanie do potrzeb

Uniwersalne rozwiązania często nie działają. Lokalne środowisko zna swoje specyficzne wyzwania.



Współodpowiedzialność

Gdy wszyscy mają poczucie wpływu i odpowiedzialności, działania są bardziej skuteczne.

Kluczowym wyzwaniem w bezpieczeństwie cyfrowym lokalnych społeczności jest budowa odporności opartej na współpracy różnych aktorów – władz, organizacji społecznych i mieszkańców. Aby ta odporność była skuteczna, potrzebna jest równość podmiotów, szybki dostęp do wiarygodnych informacji oraz wzmacnianie zaufania do instytucji.

Wspólne działanie na podstawie transparentnej, równej współpracy i zaufania stanowi fundament odporności cyfrowej lokalnych społeczności, pozwalając im lepiej reagować na zagrożenia i świadomie uczestniczyć w procesach cyfryzacji.

– Krzysztof Izdebski, Członek Zarządu Fundacji Batorego



03. Forum

Pierwsza edycja **Łowickiego Forum Bezpiecznego Internetu** odbyła się 9 października 2025 roku w Łowickim Ośrodku Kultury, inaugurując nową tradycję lokalnej edukacji i profilaktyki cyfrowej. Wydarzenie było rezultatem wielomiesięcznych przygotowań i konsultacji z różnymi środowiskami.



Struktura wydarzenia

Część I: Warsztaty

20 osób

Kameralne warsztaty "Bezpieczeństwo cyfrowe dla edukacji" z udziałem 18 kluczowych przedstawicieli środowiska edukacyjnego oraz 2 prowadzących.

Format: metoda World Café z rotacją uczestników między czterema stolikami tematycznymi.

Część II: Konferencja

~ 130 osób

Otwarta część konferencyjna z debatą panelową i wystąpieniami ekspertów, w której uczestniczyło ponad 130 osób.

Program obejmował:

- Oficjalne otwarcie przez Annę Kędziore-Zabost oraz Burmistrza Miasta Łowicza Mariusza Siewierę
- Wystąpienie Dyrektora Łowickiego Ośrodka Kultury Macieja Malangiewicza
- Dwa wystąpienia eksperckie
- Panel dyskusyjny

Część konferencyjna Forum

Wystąpienia eksperckie

- Keynote Speaker: Wojtek Kardyś

„Pato-trendy, czyli co oglądają młodzi w social mediach i co my możemy z tym zrobić”

- Dawid Adach

Siła AI – szanse, zagrożenia, rozwiązania i przyszłość cyberbezpieczeństwa”

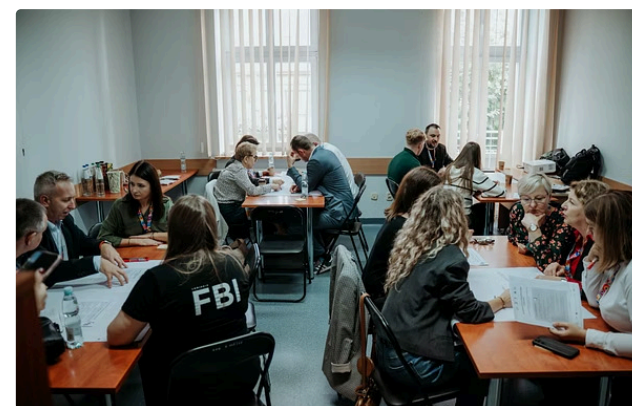
Debata panelowa:

Cyberbezpieczeństwo w lokalnej społeczności – wspólna odpowiedzialność. Uczestnicy:

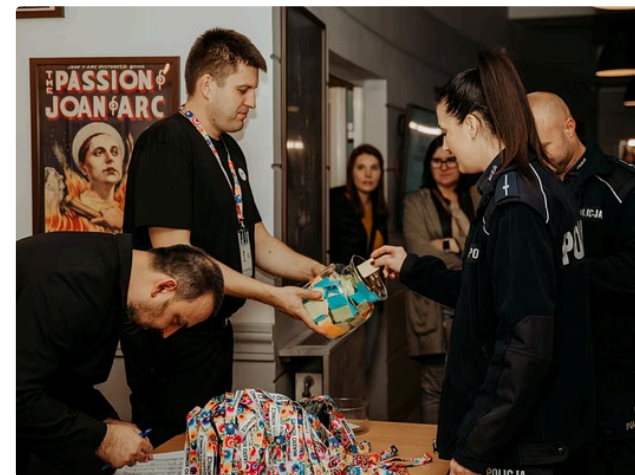
- Jacek Kłos, Zastępca Burmistrza Miasta Łowicza
- Krzysztof Izdebski, Członek Zarządu Fundacja Batorego
- Michała Brykowski, Ekspert CBZC
- Katarzyna Skierska-Pięta, Sekretarz Miasta Łowicza
- Kamil Więcek, CEO Health Soft
- Anna Kędziora-Zabost, CEO Fundacji Łowickie FBI (moderator debaty)

Forum – fotorelacja

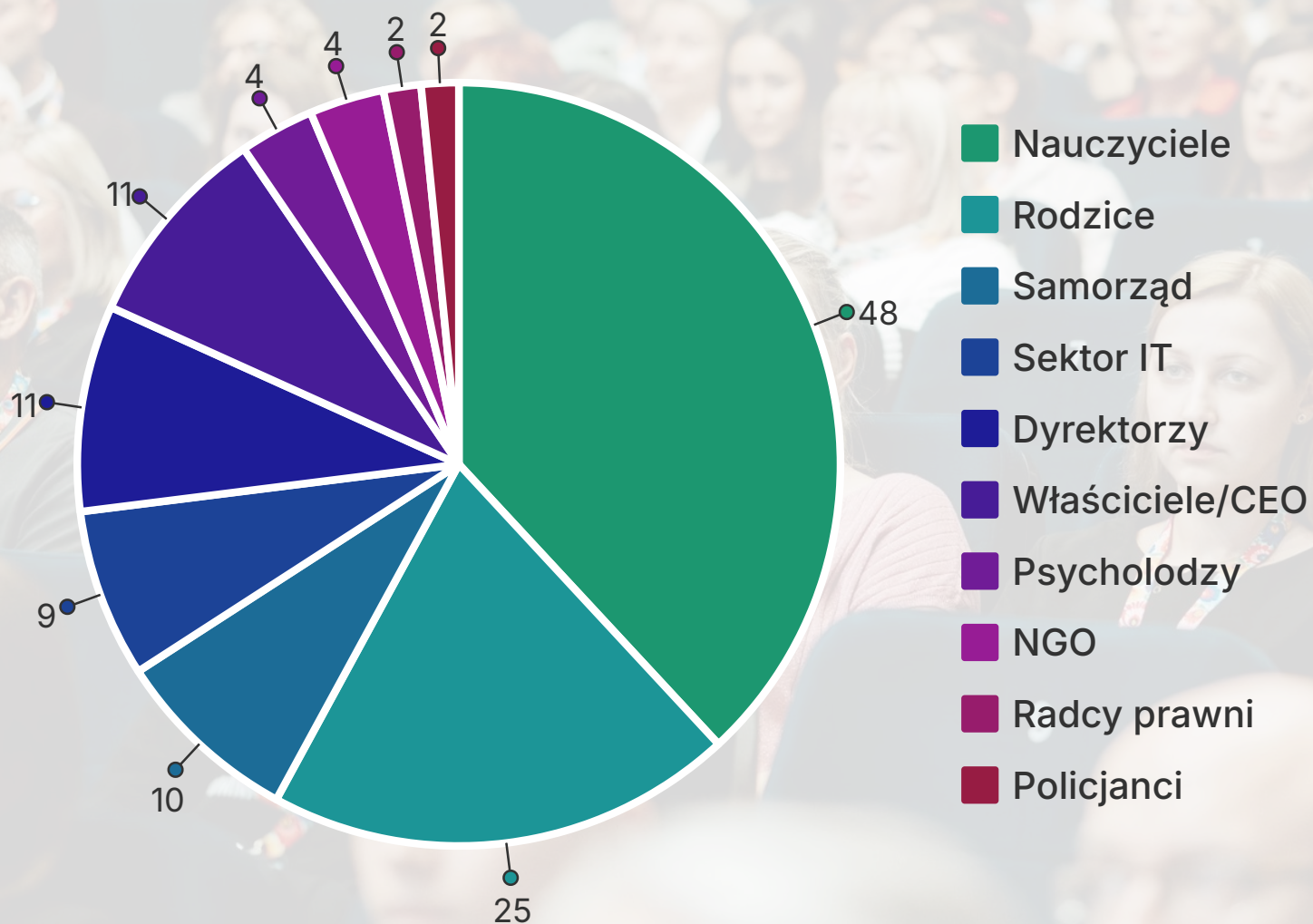
Pierwsza edycja Łowickiego Forum Bezpiecznego Internetu (od dynamicznych dyskusji panelowych, przez interaktywne warsztaty, po inspirujące wystąpienia ekspertów i rozmowy kulturalowe).



Forum – fotorelacja



Uczestnicy Forum (%) – dane z systemu rejestracji SysKonf



Prelegenci i eksperci Forum



Anna Kędziora-Zabost

CEO Fundacji
Łowickie FBI



Mariusz Siewiera

Burmistrz
Miasta Łowicza



Krzysztof Izdebski

Członek Zarządu
Fundacji Batorego



Wojtek Kardyś

Keynote speaker



Dawid Adach

Co-founder CogniVis AI



Jacek Kłos

Z-ca Burmistrza Miasta
Łowicza



**dr Katarzyna
Skierska-Pięta**

Sekretarz Miasta Łowicza



**Maciej
Malangiewicz**

Dyrektor Łowickiego
Ośrodka Kultury

Prelegenci i eksperci Forum



Michał Brykowski

Ekspert Centralnego Biura
Zwalczania
Cyberprzestępczości



Agnieszka Trzaska

Ekspertka Pracowni
Zrównoważonego Rozwoju



**Przemysław
Koper**

Ekspert w Urzędzie
Miejskim w Łowiczu



Kamil Więcek

CEO Health Soft



Hubert Kędziora

Członek Zarządu
Fundacji Łowickie FBI

Forum: wyjątkowe miejsce

Kino Fenix w dniu 9 października 2025 r. stało się miejscem wymiany wiedzy i inspiracji w zakresie higieny cyfrowej i bezpieczeństwa online.

Kultura pełni tu rolę ważnego nośnika wartości i edukacji, także w kontekście wyzwań digitalizacji, cyfryzacji oraz bezpieczeństwa w sieci – wspierając świadome i odpowiedzialne korzystanie z nowych technologii.



Łowickie Forum Bezpiecznego Internetu to niezwykle potrzebna inicjatywa otwierająca wiele szuflad, z których wychodzą współczesne zagrożenia cyfrowe. Temat nieoczywisty dla wszystkich, marginalizowany przez wielu - po kilku podanych przykładach staje się czymś wręcz szokującym. Co dalej z tym zrobimy zależy tylko od nas.

– Maciej Malangiewicz, Dyrektor Łowickiego Ośrodka Kultury



Forum: patronaty i partnerstwa merytoryczne

Organizator:



Patronaty honorowe:



MIASTO ŁOWICZ



MARSZAŁEK
WOJEWÓDZTWA ŁÓDZKIEGO
Joanna Skrzydlewska

Partnerzy merytoryczni:



Masz
Głos

I edycja Łowickiego Forum Bezpiecznego Internetu odbyła się pod Patronatem Honorowym **Marszałek Województwa Łódzkiego Pani Joanny Skrzydlewskiej** oraz **Burmistrza Miasta Łowicza Pana Mariusza Siewiery**.

Forum zyskało także wsparcie merytoryczne ogólnopolskich instytucji: **Fundacji Batorego** i **Pracowni Zrównoważonego Rozwoju** współorganizujących **Akcję Masz Głos** oraz **Centralnego Biura Zwalczania Cyberprzestępczości**.

Partnerzy I. edycji Forum:

Partnerami I edycji Forum Bezpiecznego Internetu były instytucje oraz firmy wspierające edukację cyfrową i bezpieczeństwo – w tym: firma HealthSoft.pl, Fundacja Pracownia Zrównoważonego Rozwoju, Biblioteka Miejska w Łowiczu, Łowicka Rada Biznesu, firma Zajazd Non Stop, Stowarzyszenie Wsparcie Społeczne Ja-TY-MY oraz firma SysKonf.



Partnerzy medialni pierwszej edycji Forum to: Łowicz24.eu, Radio Victoria oraz Łowiczanie.info



04. Bezpieczeństwo cyfrowe dla edukacji – warsztat

Warsztaty wykorzystały innowacyjną metodę **World Café** – dynamiczną formułę rotacyjnej dyskusji umożliwiającą poznanie różnorodnych perspektyw i wspólną syntezę pomysłów.

Czas trwania: 3h godziny



Cztery stoliki eksperckie w ramach warsztatu

#1 Diagnostyczny

Jak jest teraz?

Moderator: Hubert Kędziora, Fundacja Łowickie FBI

Analiza obecnego stanu bezpieczeństwa cyfrowego w szkołach, identyfikacja kluczowych wyzwań i obszarów wymagających interwencji.

#2 Bezpieczeństwo w szkole

Bezpieczne technologie

Moderator: Przemysław Koper, Urząd Miejski w Łowiczu

Wypracowanie standardów i procedur zapewniających bezpieczne korzystanie z technologii w środowisku szkolnym.

#3 Reagowanie na incydenty

Procedury kryzysowe

Moderator: Michał Brykowski, CBZC

Opracowanie skutecznych protokołów postępowania w sytuacjach kryzysowych związanych z cyberprzestępczością.

#4 Aktywna współpraca

Rodzice – szkoła – młodzież-samorząd

Moderator: Katarzyna Skierska-Pięta, Urząd Miasta Łowicza

Budowanie sieci współpracy i efektywnej komunikacji między wszystkimi interesariuszami.

Stolik #1 Diagnoza

Stolik diagnostyczny skupiał się na wspólnym rozpoznaniu najważniejszych wyzwań związanych z bezpieczeństwem cyfrowym w szkołach. Moderator Hubert Kędziora z Fundacji Łowickie FBI towarzyszył uczestnikom w rozmowie, zadając pytania pomagające lepiej zrozumieć obecną sytuację.



Problem: Nieświadome dzielenie się treściami

Udostępnianie bez świadomości konsekwencji

Uczniowie często publikują zdjęcia i filmy w sieci bez świadomości konsekwencji prawnych i wizerunkowych. Część z nich udostępnia cudze materiały lub tworzy własne treści o charakterze kompromitującym.

Główny problem: Przesyłane zdjęcia „zaczynają żyć własnym życiem” i stają się memami w grupach rówieśniczych. Wpływa to na zdrowie psychiczne i wykluczenie z grupy obiektów takich żartów.

Konsekwencje:

- Trwałe ślady w internecie
- Utrata kontroli nad wizerunkiem
- Ryzyko przemocy cyfrowej
- Problemy psychiczne (lęk, depresja)
- Wykluczenie społeczne



Przykład z praktyki

Jedno niefortunne zdjęcie z szatni szkolnej stało się memem w całej szkole. Uczeń przestał przychodzić na zajęcia, wymagał pomocy psychologicznej.

Problem: Wpływ sztucznej inteligencji

Technologia AI w rękach młodzieży

Nowym i szczególnie niepokojącym problemem jest wykorzystywanie sztucznej inteligencji do modyfikacji wizerunków i tworzenia fałszywych materiałów przez młodzież.

1

Brak rozróżnienia prawdy od fikcji

Dzieci i młodzież często nie odróżniają treści prawdziwych od zmanipulowanych przez AI.

2

Zalew treści generowanych przez AI

Obserwowany jest masowy napływ treści wygenerowanego przez narzędzia AI, co prowadzi do braku zaufania do wszelkich materiałów online.

3

Łatwy dostęp do narzędzi

Aplikacje do tworzenia deepfake'ów i modyfikacji zdjęć są dostępne dla każdego, często za darmo lub w atrakcyjnej cenie.

4

Brak świadomości konsekwencji prawnych

Młodzi ludzie nie zdają sobie sprawy, że tworzenie i udostępnianie fałszywych materiałów to przestępstwo.

Powiedzieć, że świat zmienia się szybciej niż kiedykolwiek to jak nie powiedzieć nic. Prawdziwe pytanie brzmi czy my zmieniamy się wystarczająco szybko?

AI to miecz obusieczny: może blokować cyberataki, ale też je tworzyć. Naszym zadaniem jest zadbać, aby przewagę miała strona dobra, dzięki inwestycji w wiedzę i odpowiedzialne praktyki.

Dawid Adach, Co-founder CogniVis AI



Problem: Brak wiedzy i refleksji

Korzystanie bez świadomości

Uczniowie korzystają z internetu i technologii cyfrowych w sposób intuicyjny, ale bez podstawowej wiedzy o mechanizmach działania sieci i konsekwencji swoich działań online.



Zasady prywatności

Młodzi użytkownicy nie rozumieją, czym jest prywatność w sieci, jak działają ustawienia prywatności i dlaczego są ważne. Często udostępniają wszystko publicznie.



Bezpieczeństwo danych

Brak wiedzy o tym, jak chronić swoje dane, hasła, konta. Słabe hasła, korzystanie z tych samych haseł w wielu miejscach, udostępnianie haseł znajomym.



Odpowiedzialność prawna

Nieświadomość konsekwencji prawnych publikowania cudzych materiałów, hejtu, szerzenia fake news. Przekonanie, że „w internecie wszystko wolno”.

Komunikacja i przepływ informacji w szkole

(bariery w komunikacji)

Uczestnicy Stolika 1 zidentyfikowali poważne problemy w komunikacji między szkołą a rodzicami oraz w przepływie informacji o incydentach cyfrowych.



Ograniczenia dziennika elektronicznego

Komunikacja z rodzicami często ogranicza się do dziennika elektronicznego (np. Librus), co nie wystarcza w przypadku poważniejszych incydentów, ale też nie jest wystarczająca do skutecznego powiadomienia np. o szkoleniu.



Rodzice w cyfrowej nieświadomości

Rodzice nie mają wiedzy o realnym życiu cyfrowym swoich dzieci – często dowiadują się o problemach z opóźnieniem z powodu stresu, przepracowania, braku zainteresowania lub bagatelizowania sygnałów.



Brak kanałów kryzysowych

Szkoła nie zawsze posiada sprawne kanały komunikacji kryzysowej, które pozwoliłyby na szybką reakcję, np. gdy występuje cyberprzemoc lub inny poważny incydent.

Zachowania uczniów (obserwacje)

Nie zgłaszają problemów

Uczniowie nie zgłaszają problemów – obawiają się reakcji dorosłych, konsekwencji, osądzenia lub braku zrozumienia. Wolą cierpieć w milczeniu.

Bezkrytyczne przesyłanie dalej

Występuje zjawisko przesyłania dalej treści kompromitujących bez refleksji nad skutkami dla ofiary. „Wszyscy to robią, więc ja też”.

Obojętność na krzywdę

Widać rosnącą obojętność na problemy rówieśników – znieczulenie na krzywdę, chęć „bycia w grupie”, lęk przed wykluczeniem jeśli ktoś zareaguje na hejt.

Potrzeba osoby zaufania

Kluczowym elementem dla skutecznego zgłaszania i reagowania na incydenty jest osoba zaufana (wychowawca, pedagog, psycholog) – ktoś, do kogo można anonimowo zgłosić się po pomoc.

Ludzie ważniejsi niż procedury

Mniej istotne są zatwierdzone procedury reagowania na incydenty; dużo ważniejsza konkretna osoba, która będzie przeszkolona i której będzie można zaufać.

- ❑ **Ważne:** To czy dana osoba jest godna zaufania musi wynikać z jej charakteru i odbioru uczniów, mniej ze sprawowanej funkcji.

Została poruszona ciekawa tematyka, bardzo ważna w dzisiejszych czasach. Swoboda wypowiedzi, możliwość rozmowy z ekspertami, połączenie sił i wymiana poglądów na dany temat. Super inicjatywa.

– Uczestnik warsztatu (anonimowa ankieta ewaluacyjna)



Rola szkoły i rodziców

Szkoła powinna

- **Aktywnie diagnozować sytuację** – prowadzić rozmowy, ankiety, monitorować nastroje uczniów
- **Organizować regularne spotkania** z rodzicami i uczniami w formie warsztatów lub debat
- **Działać prewencyjnie**, a nie tylko reagować po fakcie
- **Tworzyć przestrzeń zaufania**, gdzie uczeń wie, że może zgłosić problem bez lęku
- **Współpracować z ekspertami** i instytucjami zewnętrznymi

Rodzice potrzebują

- **Edukacji cyfrowej**, by móc współpracować ze szkołą i rozumieć wyzwania dzieci
- **Wiedzy o życiu cyfrowym dzieci** – często nie wiedzą, co się dzieje w sieci
- **Poznania języka młodzieży** i narzędzi, z których dzieci korzystają
- **Aktywnego udziału** w działaniach profilaktycznych
- **Uczenia się razem z dziećmi** – wspólne budowanie kompetencji cyfrowych

Bariery i wyzwania



Brak wspólnej definicji

Brak wspólnej definicji odpowiedzialności – kto odpowiada za co: szkoła, rodzic, dziecko? Rozmycie ról prowadzi do unikania odpowiedzialności.



Potrzeba klarownych procedur

Potrzeba jasnych procedur i reakcji w przypadku incydentów cyfrowych. Każda szkoła radzi sobie inaczej, często metodą prób i błędów.



Trudność w budowie zaufania

Trudność w zbudowaniu systemu zaufania – uczniowie nie zawsze wierzą, że zgłoszenie pomoże.



Problem z motywacją

Brak chęci uczestnictwa w działaniach profilaktycznych, szczególnie wśród rodziców. „Nie mam czasu”, „moje dziecko jest bezpieczne”.

Wnioski ze Stolika #1

Kluczowe rekomendacje diagnostyczne

Rozpoznanie realnych problemów

Potrzebne jest systematyczne rozpoznanie realnych problemów i nawyków cyfrowych w szkołach – przez rozmowy, ankiety, obserwacje. Diagnoza musi być punktem wyjścia.

Tworzenie narzędzi i procedur

Należy tworzyć narzędzia i procedury reagowania, w których szkoła, rodzic i uczeń mają jasno określone role i wiedzą, czego mogą się od siebie nawzajem oczekiwać.

Współpraca z ekspertami

Szkoła powinna regularnie współpracować z ekspertami i instytucjami (np. NASK, policja, psycholodzy), aby lepiej diagnozować sytuacje i skutecznie reagować.

Zmiana narracji

Trzeba zmienić narrację z kontrolnej na wspierającą – budować relację zaufania zamiast strachu. Tylko wtedy uczniowie będą zgłaszać problemy.

Działania profilaktyczne

Diagnoza musi być punktem wyjścia do opracowania skutecznych działań profilaktycznych i edukacyjnych dostosowanych do rzeczywistych potrzeb.

Stolik #2: Rola szkoły w zakresie bezpieczeństwa cyfrowego

Drugi stolik warsztatowy koncentrował się na wypracowaniu konkretnych rozwiązań dla środowiska szkolnego. Moderator Przemysław Koper z Urzędu Miejskiego w Łowiczu prowadził dyskusję z perspektywy praktycznej implementacji bezpieczeństwa cyfrowego w szkołach.



Główne obserwacje i problemy

Bezpieczeństwo w szkole



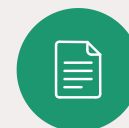
Brak informacji w szkole

Brakuje jasnych, łatwo dostępnych procedur i informacji o tym, jak reagować w przypadku incydentu. Uczniowie często nie wiedzą, do kogo mogą się zwrócić po pomoc.



Współpraca z rodzicami

Szkoła powinna rozwijać regularną współpracę z rodzicami w zakresie bezpieczeństwa cyfrowego poprzez spotkania informacyjne i warsztaty.



Potrzeba ujednolicenia

Obecnie każda szkoła reaguje inaczej – brak jednolitych wytycznych. Należy opracować procedurę reagowania na incydenty obowiązującą wszystkie placówki.

Uczestnicy podkreślali, że potrzebny jest **systemowy model reagowania**, który byłby zrozumiały dla uczniów, nauczycieli i rodziców, a jednocześnie wystarczająco elastyczny, by uwzględniać specyfikę poszczególnych szkół.

Rekomendacje praktyczne

Działania do wdrożenia: spotkania z rodzicami, wspólne inicjatywy uczniów i szkoły

Zwiększyć częstotliwość zebrań dotyczących bezpieczeństwa cyfrowego i włączać w nie ekspertów z zakresu cyberbezpieczeństwa. Angażować uczniów w tworzenie kampanii profilaktycznych – uczniowie chętniej reagują, jeśli mają poczucie sprawczości.

Proponowane działania:

- Warsztaty dla Rodziców (uświadamiające z jakimi zagrożeniami mierzą się dzieci)
- Zapraszanie ekspertów (NASK, policja, fundacje edukacyjne)
- Warsztaty praktyczne (jak wykorzystać nową technologię w celu ochrony dzieci)
- Wymiana doświadczeń między rodzicami
- Akcje i kampanie szkolne organizowane przez samorząd uczniowski
- **Peer education – starsi uczniowie edukujący młodszych**



Praca z wychowawcami i pedagogami

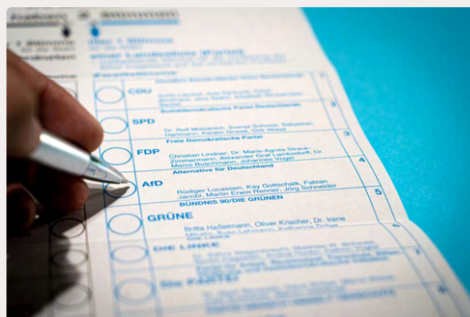
Narzędzia dla kadry pedagogicznej

Wychowawcy i pedagodzy muszą mieć jasne narzędzia do reagowania oraz przejść szkolenie z komunikacji kryzysowej.



Szkolenia dla nauczycieli

Regularne szkolenia z zakresu komunikacji kryzysowej, rozpoznawania sygnałów ostrzegawczych i psychologicznych aspektów reagowania na incydenty.



Gotowe narzędzia

Formularze zgłoszeniowe, listy kontaktowe do instytucji pomocowych, przykłady scenariuszy działań w różnych sytuacjach, checklisty postępowania.



Rozpoznawanie sygnałów

Każdy nauczyciel powinien wiedzieć, jak rozpoznać pierwsze sygnały problemu: wycofanie ucznia, wzrost nieobecności, zmiany zachowania, unikanie kontaktów.

Antycypowanie zagrożeń

Reagowanie zanim dojdzie do incydentu

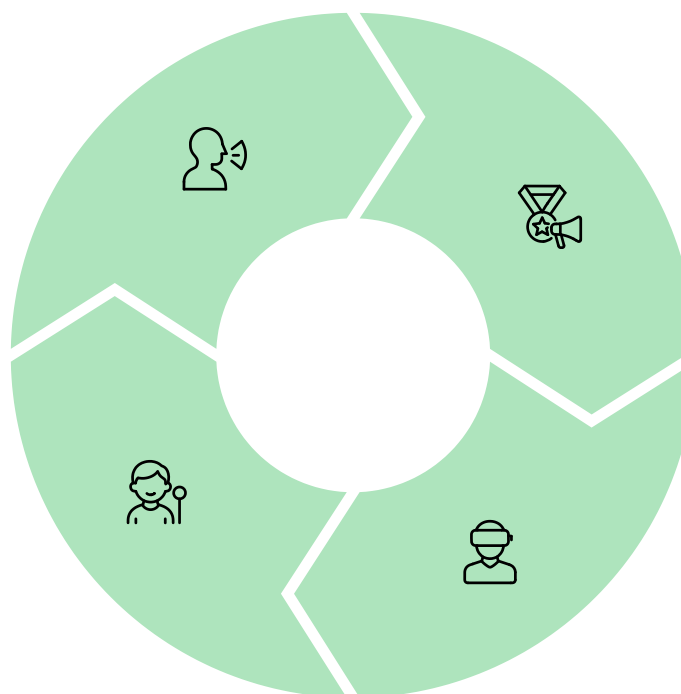
Kluczowe jest działanie proaktywne – budowanie atmosfery zaufania i edukacja prewencyjna, zanim wystąpi problem.

Regularne rozmowy

Prowadzenie regularnych rozmów o bezpieczeństwie cyfrowym na godzinach wychowawczych

Wczesne wykrywanie

Aktywne monitorowanie nastrojów i relacji w klasie



Atmosfera zaufania

Tworzenie środowiska, gdzie uczeń nie boi się zgłosić problemu

Symulacje

Gry anty-hejterskie i scenariusze symulacyjne uczące reakcji w bezpiecznych warunkach

Powiązanie z systemem wychowawczym

Integracja z programem szkoły

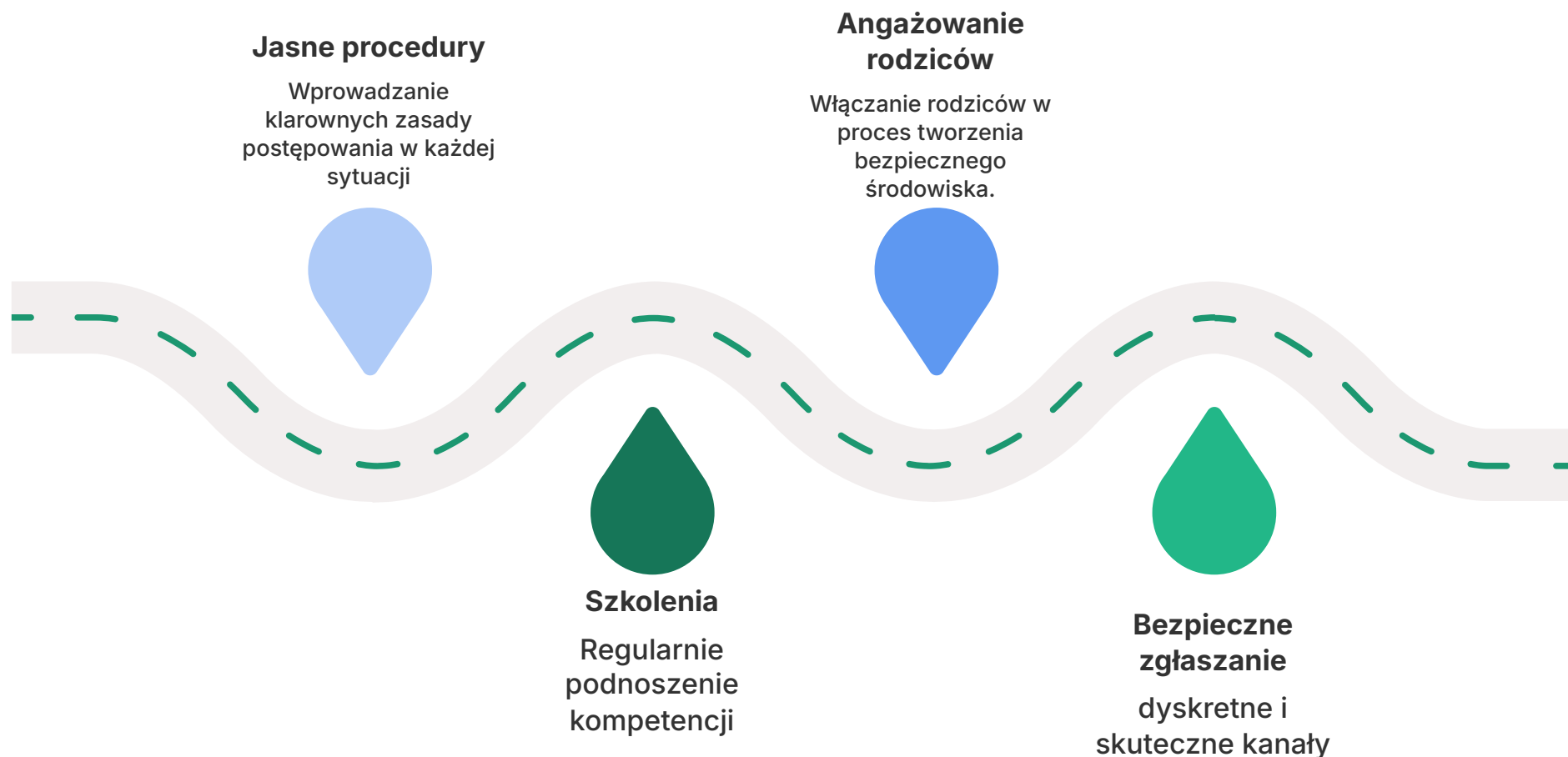
Tematyka reagowania na incydenty powinna być częścią programu wychowawczo-profilaktycznego szkoły, a nie odrębną inicjatywą.

Przedmiot	Sposób integracji
Informatyka	Bezpieczne korzystanie z internetu, skuteczna ochrona danych oraz rozpoznawanie cyfrowych zagrożeń, a także aktywne angażowanie uczniów we wspólne dzielenie się własnymi doświadczeniami i pomysłami na mitygowanie ryzyka online
WOS	Prawa i obowiązki w Internecie, odpowiedzialność prawna, etyka cyfrowa
Etyka	Cyfrowa empatia, konsekwencje działań online, odpowiedzialność za słowo
Godzina wychowawcza	Regularne dyskusje o sytuacjach w klasie, scenariusze problemowe, aktywne angażowanie uczniów we wspólne dzielenie się doświadczeniami
Projekty tematyczne	Długofalowe inicjatywy edukacyjne, kampanie profilaktyczne



Regularne rozmowy i projekty tematyczne mogą zapobiec poważniejszym incydomom

Wnioski ze Stolika #2



- ❏ Reakcja na incydenty nie powinna być jednorazowym działaniem, lecz stałym elementem kultury bezpieczeństwa szkoły. Kluczowe jest, by szkoła aktywnie budowała otwartość wśród uczniów – zachęcała ich do dzielenia się własnym doświadczeniem, zwłaszcza poprzez wsparcie starszych kolegów oraz absolwentów. Efektywność działań zależy od przejrzystej komunikacji, współpracy z rodzicami i zaangażowania kadry wychowawczej.



Stolik #3: Reagowanie na incydenty

Perspektywa instytucjonalna

Trzeci stolik warsztatowy prowadzony przez komisarza Michała Brykowskiego z Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) koncentrował się na aspektach proceduralnych i instytucjonalnych reagowania na incydenty cyfrowe.



Procedura reagowania na incydenty

Propozycja struktury

1

Zgłoszenie problemu

Jasny schemat: uczeń → nauczyciel/osoba zaufania → wychowawca → pedagog → dyrekcja.
Możliwość zgłoszenia anonimowego.

2

Rola wychowawcy

Pierwsza linia kontaktu, ocena sytuacji, podjęcie działań wstępnych, informowanie pedagoga i dyrekcji.

3

Rola pedagoga i psychologa

Wsparcie emocjonalne, rozmowa z uczniem poszkodowanym i sprawcą, pomoc w rozwiązaniu konfliktu.

4

Rola dyrekcji

Podejmowanie decyzji o dalszych krokach, kontakt z rodzicami, ewentualnie ze służbami (policja, prokuratura).

5

Działania następne

Rozmowa z zaangażowanymi stronami, wsparcie dla ofiary, konsekwencje dla sprawcy, dokumentacja, monitorowanie sytuacji.

6

Komunikacja z rodzicami

Informowanie rodziców ucznia poszkodowanego i sprawcy, wspólne ustalenie dalszych działań.



Procedura powinna być umieszczona w widocznym miejscu: gabloty, strona szkoły, dziennik elektroniczny.

Problem: Brak informacji o zgłaszaniu

Gdzie zgłaszać incydenty?

W wielu przypadkach brak jest jasnych procedur i wiedzy wśród uczniów, nauczycieli czy rodziców, do kogo należy zgłaszać incydenty dotyczące bezpieczeństwa w sieci.



dyzurnet.pl

NASK - krajowy punkt kontaktowy zajmujący się reagowaniem na nielegalne treści w Internecie



CERT Polska

NASK - Właściwy w przypadkach incydentów technicznych (phishing, malware, fałszywe domeny)



Telefon zaufania

116 111 - Kontakt pomocowy dla młodzieży w sytuacjach zagrożeń psychicznych lub emocjonalnych



Numer alarmowy 112

112 - sytuacje wymagające natychmiastowej interwencji służb ratunkowych lub policji



Wniosek: Należy zapewnić dostępność i widoczność tych informacji w każdej placówce edukacyjnej (gabloty, strony szkół, e-dzienniki).

Brak uregulowań prawnych

Uczestnicy Stolika 3 zidentyfikowali poważny problem: brak jednolitych, obowiązujących w całej Polsce regulacji dotyczących reagowania na incydenty cyfrowe w środowisku szkolnym.

Obecny stan

- Każda szkoła interpretuje przepisy inaczej
- Brak jasnych wytycznych ministerialnych
- Różne podejścia do podobnych incydentów
- Niepewność prawna nauczycieli i dyrektorów

Potrzebne regulacje

- Ujednolicenie przepisów na poziomie ministerialnym
- Wprowadzenie zapisów w statutach szkół
- Jasne określenie odpowiedzialności
- Standardy współpracy z instytucjami

Takie uregulowania powinny jasno określać:

- ☐ Kto odpowiada za przyjmowanie zgłoszeń?
- ☐ W jaki sposób reaguje się na incydenty?
- ☐ Jakie działania podejmuje szkoła wobec sprawców i osób poszkodowanych?
- ☐ Jak współpracuje z instytucjami zewnętrznymi (NASK, policja, poradnie psychologiczne)?

Zasady korzystania z urządzeń w szkole

Zasugerowano, by w statucie każdej szkoły znalazł się zapis dotyczący zasad korzystania z telefonów komórkowych i innych urządzeń cyfrowych.

Warunki dopuszczalnego użycia

Określenie sytuacji, w których można korzystać z urządzeń (np. cele edukacyjne, za zgodą nauczyciela)

Współodpowiedzialność uczniów

Jasne zasady odpowiedzialności za przestrzeganie regulaminu oraz konsekwencje ich łamania.

- ❑ Ważne jest, aby regulamin powstał we współpracy z uczniami i rodzicami, a nie został im narzucony odgórnie – zwiększa to akceptację i przestrzeganie zasad.



Odpowiedzialność i kanały komunikacji

Wskazano, że w strukturze szkoły osoby odpowiedzialne za przyjmowanie zgłoszeń i reagowanie na incydenty powinny być jasno wyznaczone i znane całej społeczności szkolnej.



Wychowawca

Pierwszy punkt kontaktu dla uczniów – osoba, której uczniowie ufają i która zna sytuację w klasie



Skrzynki zaufania

Fizyczne lub elektroniczne, pozwalające uczniom bezpiecznie i anonimowo zgłaszać problemy



Pedagog/psycholog

Wsparcie emocjonalne i interwencja w przypadkach przemocy – profesjonalna pomoc psychologiczna



Anonimowe maile

Alternatywny kanał dla uczniów niechących rozmawiać osobiście – możliwość zgłoszenia online

Rekomendujemy opracowanie długofalowej strategii budowania bezpieczeństwa cyfrowego na poziomie lokalnym w odniesieniu do konkretnych placówek - np. szkolnych, zawierającą zarówno ogólne kierunki jak i konkretne, możliwe do wdrożenia w najbliższej przyszłości działania (np. warsztaty z młodzieżą, wspólnie wypracowane regulaminy higieny cyfrowej w szkole). Kluczowa jest międzysektorowa współpraca.

– Agnieszka Trzaska, Ekspertka Pracowni Zrównoważonego Rozwoju



Infrastruktura techniczna

W końcowej części dyskusji pojawiły się kluczowe postulaty dotyczące infrastruktury i bezpieczeństwa technicznego w szkołach, mające na celu zapewnienie bezpiecznego środowiska cyfrowego.

Infrastruktura sieciowa z filtrowaniem

Wdrożenie zaawansowanych systemów filtrujących, które skutecznie blokują treści niepożądane w sieci szkolnej. Dotyczy to w szczególności:

- ☐ Pornografii i treści erotycznych
- ☐ Przemocy i brutalnych materiałów
- ☐ Hazardu i gier losowych
- ☐ Nielegalnych stron internetowych
- ☐ Potencjalnie niebezpiecznych witryn

Finansowanie i wsparcie dla wdrożeń

Zwrócono uwagę na konieczność zabezpieczenia odpowiednich środków finansowych na wdrożenie i utrzymanie powyższych rozwiązań. Brak funduszy jest obecnie główną barierą.

Szkoły potrzebują kompleksowego wsparcia finansowego, które obejmuje zarówno zakup i instalację infrastruktury technicznej, jak i szkolenia kadry nauczycielskiej oraz rozwój programów edukacyjnych dla uczniów w zakresie cyfrowego bezpieczeństwa.

Wnioski ze Stolika #3

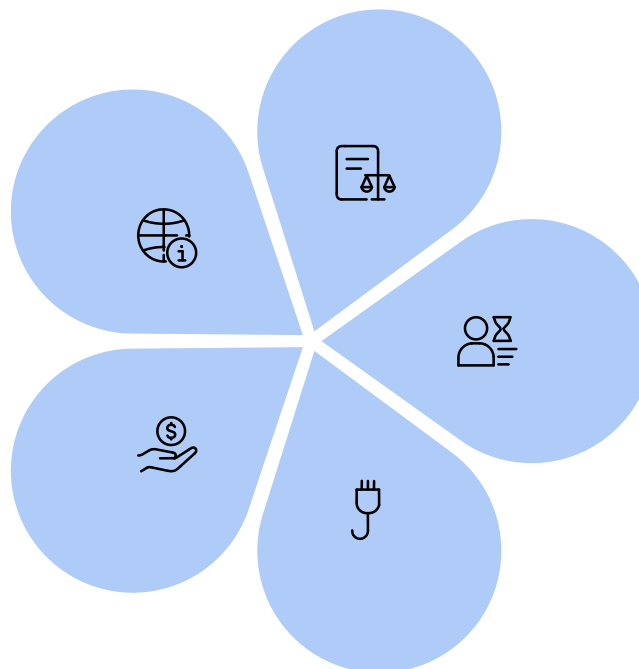
Rozmowy przy Stolicu 3 wskazały na potrzebę **zintegrowanego podejścia do reagowania na incydenty w środowisku szkolnym**, łączącego aspekty prawne, organizacyjne i techniczne.

Edukacja i komunikacja

Jasne instrukcje, gdzie zgłaszać incydenty

Zapewnienie finansowania

Środki na rozwiązania techniczne i szkolenia



Ujednolicenie przepisów

Wprowadzenie zapisów do statutów szkół

Wyznaczenie odpowiedzialnych

Stworzenie bezpiecznych kanałów zgłaszania

Infrastruktura techniczna

Wzmocnienie zabezpieczeń sieciowych

- ☐ Tylko kompleksowe podejście uwzględniające wszystkie te elementy może zapewnić skuteczne bezpieczeństwo cyfrowe w szkołach.



Stolik 4: Aktywna współpraca

Rodzice – szkoła – młodzież – instytucje

Czwarty stolik warsztatowy prowadzony przez Katarzynę Skierską-Pietę Sekretarz Urzędu Miasta Łowicza koncentrował się na budowaniu efektywnej sieci współpracy między wszystkimi interesariuszami procesu edukacji i bezpieczeństwa cyfrowego.

Rola rodziców

Rodzice odgrywają kluczową rolę w kształtowaniu świadomości cyfrowej i bezpieczeństwa młodzieży. Wyróżniono trzy podstawowe postawy rodzicielskie, z których każda ma swoje zalety i ograniczenia.

Trzy postawy rodzicielskie

Kontrolująca

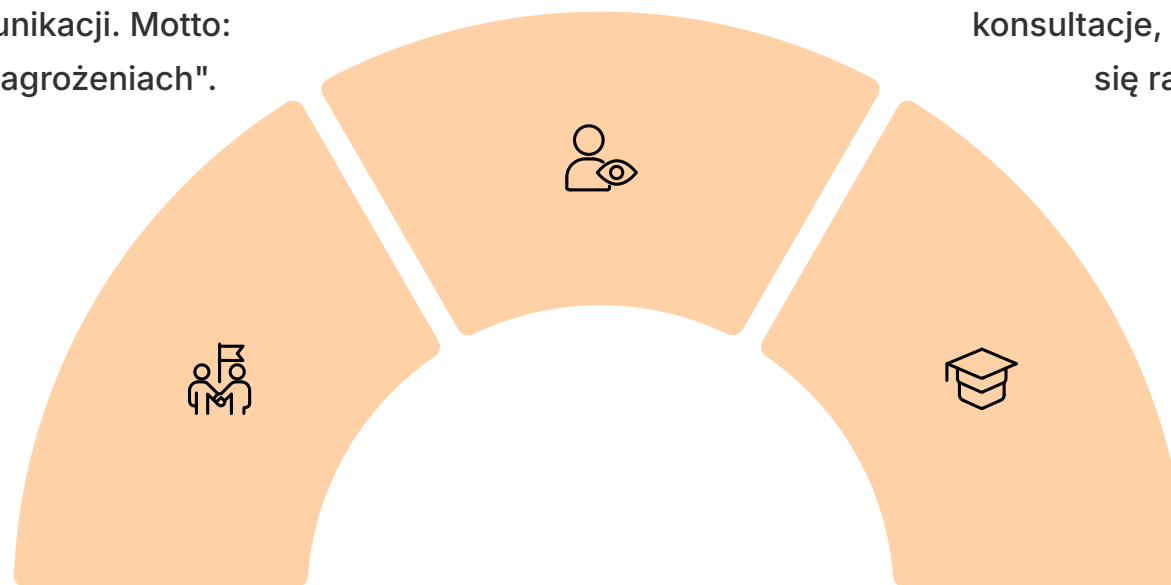
Rodzic sprawdza czas spędzany w sieci, kontroluje treści i kontakty dziecka, stosuje narzędzia kontroli rodzicielskiej i monitoringu.

Wspierająca

Rodzic ufa dziecku, rozmawia o zagrożeniach, buduje relację opartą na zaufaniu i otwartej komunikacji. Motto: „Ufam i rozmawiam o zagrożeniach”.

Profilaktyczna

Rodzic angażuje się w działania profilaktyczne szkoły (warsztaty, konsultacje, akcje informacyjne), uczy się razem z dzieckiem.



- ❑ **Wnioski:** Najlepsze efekty daje połączenie postawy **wspierającej i edukacyjnej** – opartej na rozmowie i wspólnym uczeniu się, a nie wyłącznie na kontroli.

Jak angażować rodziców i wspierać szkoły?

01

Motywowanie rodziców

- Organizuj praktyczne warsztaty i symulacje.
- Wykorzystaj "efekt rówieśniczy" – rodzic uczy rodzica.

02

Systemowe wsparcie szkół

- Zapewnij stałą współpracę z placówkami oświatowymi, policją i samorządem.
- Włączaj szkoły w ogólnopolskie programy profilaktyczne.

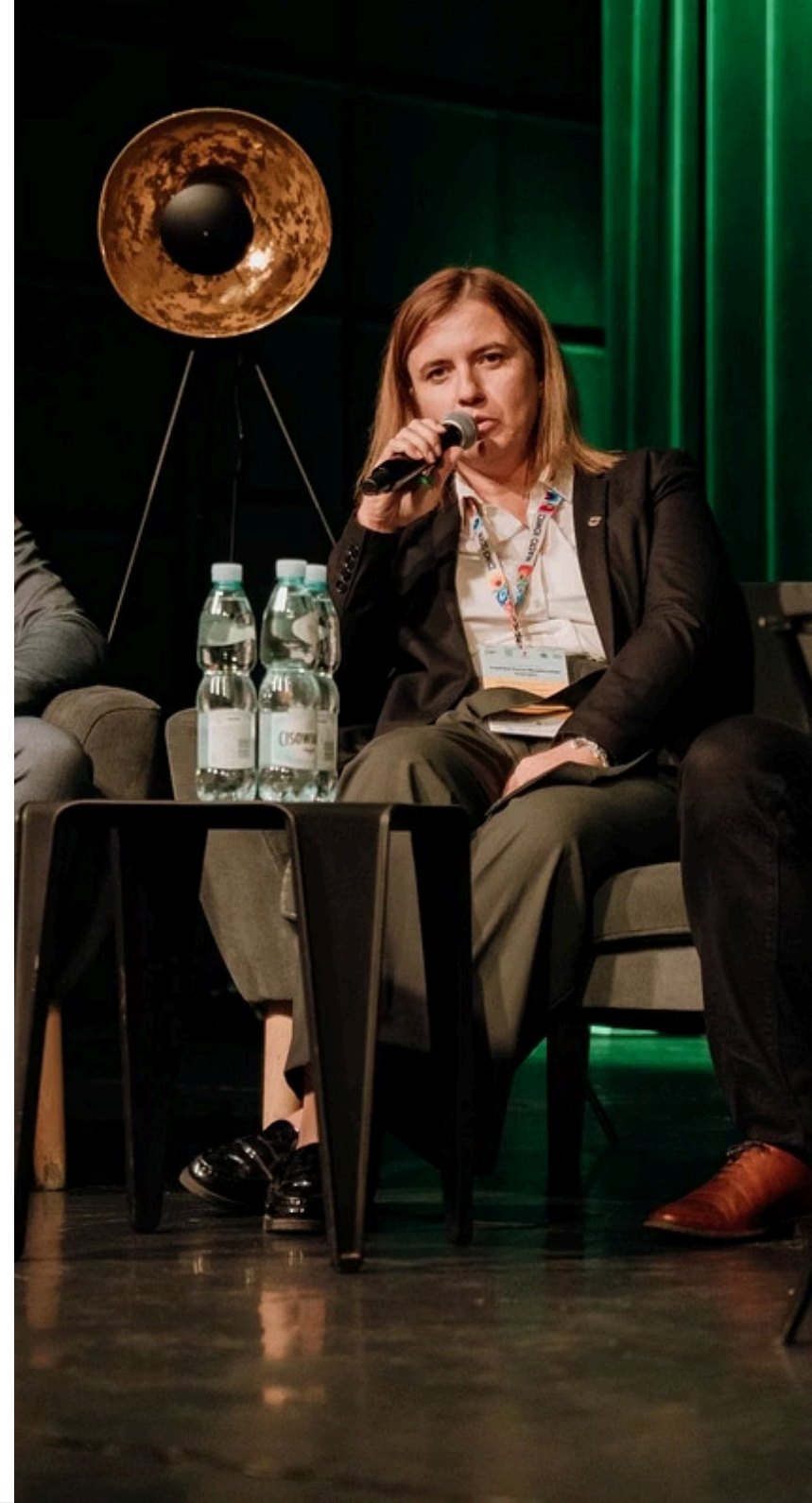
03

Nowoczesny przekaz

- Używaj AI do tworzenia interaktywnych form edukacyjnych (quizy, filmy).
- Wykorzystuj media społecznościowe i platformy cyfrowe.

Nawet najbardziej nowoczesna technologia nie zastąpi człowieka. Dlatego tak ważne jest, aby skupić się nie tylko na jej unowocześnianiu, czy wzmacnianiu różnego rodzaju procedur, ale także na człowieku, wzmacnianiu jego kompetencji i działaniom służącym podnoszeniu jego kwalifikacji.

– Katarzyna Skierska-Pięta, Sekretarz Urzędu Miejskiego w Łowiczu



Główne rekomendacje ze Stolika #4

Warsztaty lokalne

- Wspólne zajęcia dla uczniów, rodziców i nauczycieli.
- Badanie sprawności cyfrowej.
- Edukacja cyfrowa w programie wychowawczym.

Kampanie społeczne

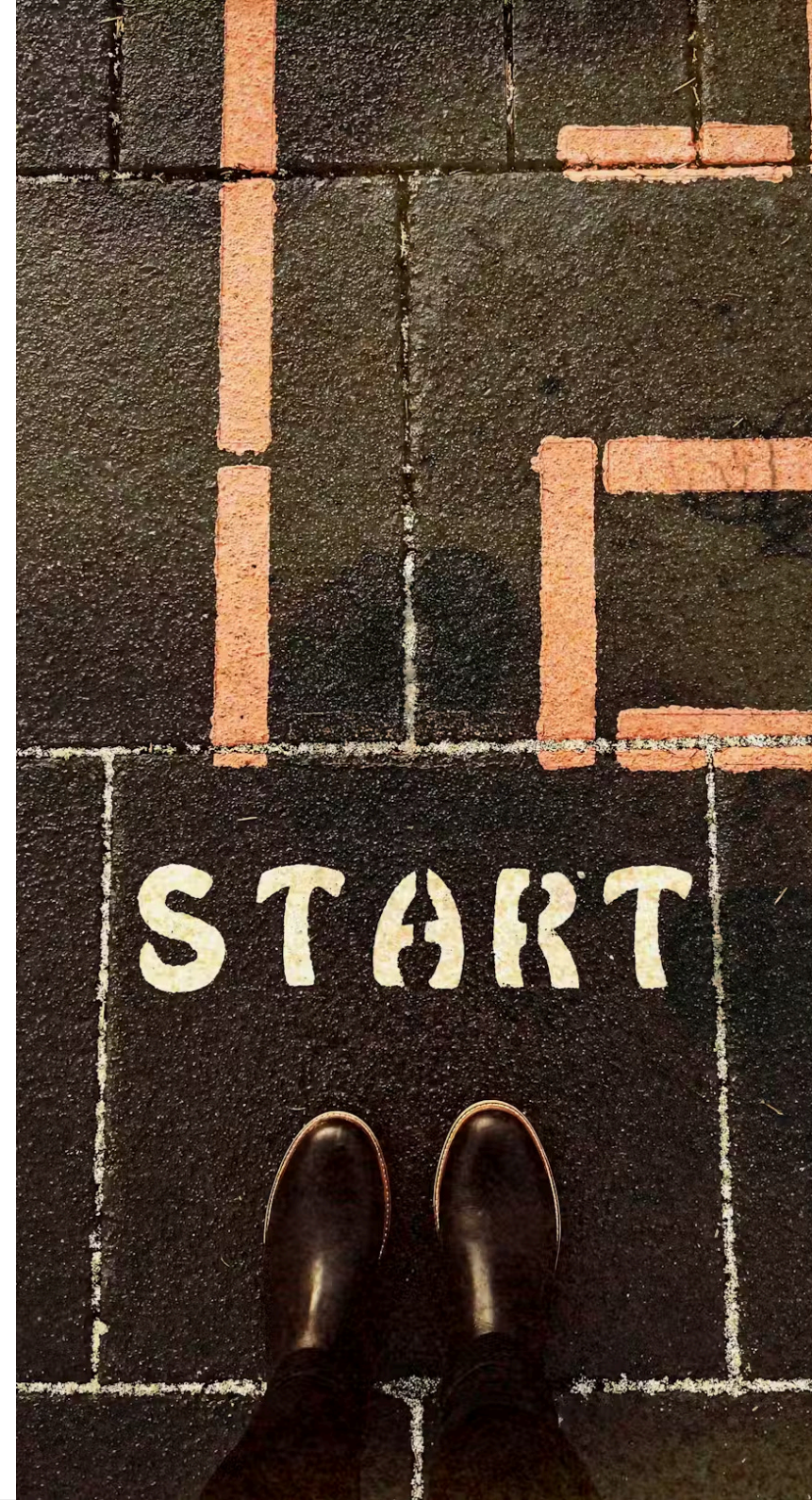
- Promowanie pozytywnych wzorców korzystania z Internetu.
- Pokazywanie dobrych praktyk online.
- Szkoła oferuje atrakcyjne alternatywy dla czasu przed ekranem.

Współpraca z ekspertami

- Wykorzystanie zasobów NASK i NGO's
- Wsparcie psychologów (cyberprzemoc).
- Pomoc mediatorów (rozwiązywanie konfliktów, relacje w sieci).

📌 **Kluczowe przesłanie:** Budujemy zaufanie, nie kontrolę – to fundament bezpieczeństwa cyfrowego! Działania oparte na otwartości przyniosą trwalsze efekty niż zakazy.

04. Wnioski ogólne



Główne wnioski po I. edycji Forum



Skuteczna współpraca

Potwierdzono efektywność międzysektorowej współpracy (władze, szkoły, rodzice, młodzież, eksperci).



Lokalny wymiar wyzwań

Uświadomienie, że globalne wyzwania cyfrowe mają realny, lokalny wymiar.



Wzrost świadomości edukacyjnej

Podkreślono kluczową rolę ciągłej edukacji cyfrowej dla wszystkich grup społecznych.



Waga zaufania nad kontrolą

Zidentyfikowano, że otwarta komunikacja i zaufanie są skuteczniejsze niż restrykcyjne zakazy.



Wspólna odpowiedzialność

Ugruntowano poczucie wspólnej odpowiedzialności społeczności za bezpieczne środowisko cyfrowe.

Rekomendacje systemowe

Kluczowe działania do wdrożenia lokalnie



Długofalowa strategia cyfrowa

Opracowanie i wdrożenie standardów bezpieczeństwa cyfrowego dla placówek edukacyjnych i całej społeczności.



Cykliczne szkolenia i warsztaty

Organizowanie regularnych szkoleń dla uczniów, rodziców i nauczycieli, zwiększających świadomość i uczących bezpiecznych praktyk.



Procedury reagowania kryzysowego

Opracowanie i wdrożenie jasnych procedur reagowania na incydenty cyfrowe (np. cyberprzemoc) w szkołach).



Diagnoza kompetencji cyfrowych

Regularne badanie poziomu wiedzy cyfrowej mieszkańców, dla lepszego dopasowania programów edukacyjnych.



Wzmacnianie współpracy międzysektorowej

Budowanie partnerstw między szkołami, samorządem, policją, NASK i NGO dla efektywnej synergii działań.

06

Utworzenie grupy roboczej

Grupa robocza, która omówi i doprecyzuje rekomendacje wypracowane podczas Forum oraz możliwy tryb ich wdrożenia w placówkach edukacyjnych w Łowiczu.

06. Edukacja

– czyli fundament bezpieczeństwa
naszej lokalnej społeczności



Fundamentem bezpieczeństwa cyfrowego jest edukacja. Potrzebne są kompleksowe programy dla wszystkich grup wiekowych – dzieci, rodziców, nauczycieli oraz seniorów.

Edukacja cyfrowa na stałe

- Integracja higieny cyfrowej w programach szkolnych.
- Nauka rozpoznawania zagrożeń online dla młodych i seniorów (phishing, fake newsy).
- Kształtowanie bezpiecznych oraz odpowiedzialnych zachowań w sieci.

Warsztaty dla wszystkich grup

- Dla młodzieży/seniorów: praktyczne scenariusze i symulacje.
- Dla rodziców: zrozumienie świata online dziecka, narzędzia wsparcia.
- Dla nauczycieli: procedury reagowania i wykorzystanie narzędzi cyfrowych.

Nowoczesne technologie i AI

- Wykorzystanie interaktywnych quizów, filmów i symulacji zagrożeń.
- Personalizacja treści edukacyjnych z użyciem AI.
- Dostosowanie języka do odbiorców (np. młodzieży czy seniorów).

Te kluczowe działania stworzą silny fundament wiedzy i umiejętności cyfrowych.

Największym wyzwaniem jest dziś dostosowanie firm i samorządów do wymagań NIS2, edukacja rodziców i dzieci w zakresie bezpiecznego korzystania z technologii oraz świadome spędzanie czasu razem – zamiast przed ekranem.

– Kamil Więcek, CEO HealthSoft





07. Dalsze kroki

Pilotaż w szkole podstawowej w Łowiczu

- ❏ W ramach budowania cyfrowej odporności Fundacja planuje wraz z Urzędem Miasta Łowicza pilotaż wypracowanych standardów i rozwiązań w wybranej szkole podstawowej w Łowiczu. Celem jest praktyczne wdrożenie i testowanie rekomendacji po Forum oraz podniesienie świadomości i bezpieczeństwa cyfrowego wśród uczniów, rodziców i kadry pedagogicznej.

Wybrane elementy pilotażu:

1

Warsztaty dla najmłodszych

Specjalnie zaprojektowane warsztaty dla klas 1–3, skupiające się na podstawach bezpieczeństwa online i zdrowych nawykach cyfrowych.

2

Szkolenia dla dorosłych

Szkolenia i zajęcia dla nauczycieli i rodziców, wspierające ich w rozpoznawaniu zagrożeń cyfrowych i reagowaniu na incydenty.

3

Procedury reagowania na incydenty

Wdrożenie i testowanie jasnych i efektywnych procedur reagowania na cyberprzemoc, hejt czy niebezpieczne treści.

Młodzi Liderzy Cyberbezpieczeństwa (pilotaż)

Młodzi Liderzy Cyberbezpieczeństwa to pomysł Fundacji Łowickie FBI na program szkoleniowy i mentoringowy, którego celem będzie przygotowanie wybranych uczniów szkół średnich w Łowiczu do roli liderów cyfrowych w swojej społeczności rówieśniczej.

- ❏ Projekt opiera się na idei edukacji młodych ludzi oraz wsparciu ich w projektowaniu i realizacji różnych oddolnych inicjatyw z zakresu higieny cyfrowej i bezpieczeństwa online.



Rekrutacja grupy

zaangażowani uczniowie z predyspozycjami przywódczymi



Szkolenia, warsztaty, spotkania

tematyka: bezpieczeństwo i higiena cyfrowa



Współpraca

Młodzież, Szkoła, Fundacja, władze samorządowe



Wspólne akcje oraz inicjatywy szkolne

we współpracy z Fundacją

Dalsze kroki Fundacji

Łowickie Forum Bezpiecznego Internetu to długofalowa inicjatywa. Poniżej przedstawiamy kluczowe kierunki rozwoju i plany, mające na celu dalsze wzmacnianie cyfrowej odporności lokalnej społeczności.



Kontynuacja i rozwój Forum

Cykliczne edycje Forum
z rozszerzonym zakresem
tematycznym

**Cel: angażowanie szerszego grona
uczestników.**



Wdrażanie rekomendacji

Przekucie rekomendacji po Forum
w działania pilotażowe w szkołach
podstawowych
i ponadpodstawowych. Poprawa
bezpieczeństwa cyfrowego uczniów,
rodziców i nauczycieli.



Partnerstwa i współpraca

Wymiana doświadczeń z innymi
miastami i podmiotami w Polsce, udział
w ogólnopolskich programach dla
wzmocnienia pozycji Łowicza w
obszarze bezpieczeństwa cyfrowego;
pozyskiwanie grantów, dotacji oraz
sponsorów na działania edukacyjne
i profilaktyczne w Łowiczu i regionie.



Kluczowe przesłanie: "Bezpieczeństwo cyfrowe to długofalowy proces. Budujmy je razem – krok po kroku!"

Łączymy siły dla cyfrowego bezpieczeństwa regionu

– zostań darczyńcą, wspieraj nasze działania.



Fundacja Łowickie Forum Bezpiecznego Internetu

www.lowickiefbi.pl

