

RAPORT ANALITYCZNY / ANALYTICAL REPORT

Bezpieczne kompetencje cyfrowe młodych ludzi w Polsce

Analiza danych GUS i raportów publicznych dla działań edukacyjnych
Fundacji Obywatele Przyszłości w latach 2026-2027

Fundacja Obywatele Przyszłości
KRS 0001041967 | Michałowice / Kraków

Lipiec 2026 / July 2026

95,9%

gospodarstw domowych
z dostępem do internetu
w 2024 r.

48,8%

osób 16-74 z co najmniej
podstawowymi
kompetencjami
cyfrowymi

**600
tys.+**

zgłoszeń cyberzagrożeń
do CERT Polska w 2024 r.

CEL DOKUMENTU / PURPOSE

Jak czytać ten raport / How to read this report

Cel raportu. Dokument przedstawia modelową analizę przygotowaną przez Fundację Obywatele Przyszłości na podstawie publicznie dostępnych danych GUS, raportów rządowych i opracowań instytucji publicznych. Raport pokazuje, dlaczego edukacja cyfrowa młodych ludzi powinna być łączona z bezpieczeństwem, odpornością informacyjną i kompetencjami obywatelskimi.

Zakres. Analiza obejmuje: dostęp do internetu, poziom kompetencji cyfrowych, lukę w obszarze bezpieczeństwa cyfrowego młodych osób, dynamikę cyberzagrożeń oraz kierunki polityk publicznych na lata 2026-2027.

Charakter. To opracowanie własne typu desk research. Dane liczbowe nie są audytem ani badaniem pierwotnym Fundacji; zostały zrekapitulowane i zinterpretowane w kontekście projektów edukacyjnych, akademickich i obywatelskich.

Report objective. This document presents a model analytical report prepared by the Future Citizens Foundation using public data from Statistics Poland, government reports and public-sector institutions. It explains why digital education for young people should be integrated with safety, information resilience and civic competencies.

Scope. The analysis covers internet access, digital skills, the digital safety gap among young people, the dynamics of cyber threats and public-policy priorities for 2026-2027.

Type of document. This is an original desk-research analysis. The numerical data are not a primary survey by the Foundation; they are public indicators interpreted for educational, academic and civic project design.

Teza raportu / Main thesis

W Polsce problemem nie jest już wyłącznie dostęp do technologii. Kluczowym wyzwaniem staje się jakość korzystania z technologii: bezpieczeństwo cyfrowe, odporność na oszustwa i dezinformację, odpowiedzialne użycie AI oraz zdolność młodych osób do działania w środowisku informacyjnym.

Spis treści / Contents

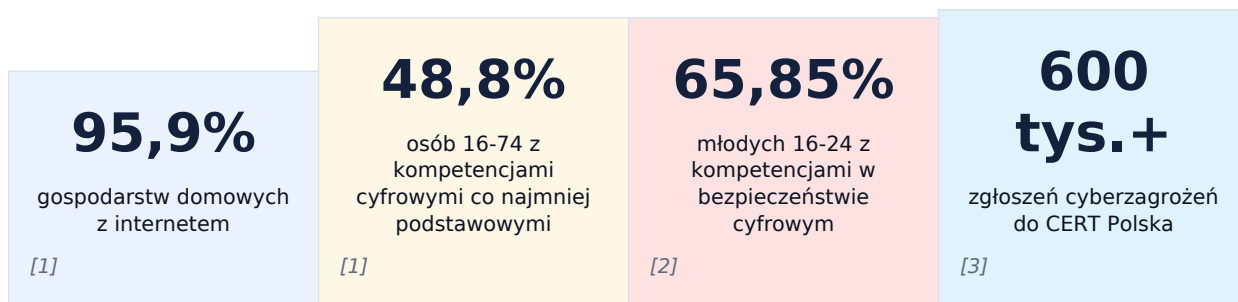
1. Część polska: główne wnioski, dane, diagnoza, rekomendacje
2. English section: executive summary, data snapshot, diagnosis, recommendations
3. Metodologia, ograniczenia i źródła publiczne / Methodology, limitations and public sources

CZĘŚĆ POLSKA

Streszczenie zarządcze

Publiczne dane z lat 2023-2025 pokazują wyraźną rozbieżność między powszechnym dostępem do technologii a jakością kompetencji cyfrowych. W 2024 r. dostęp do internetu posiadało 95,9% gospodarstw domowych, natomiast odsetek osób w wieku 16-74 lata posiadających podstawowe lub ponadpodstawowe umiejętności cyfrowe wyniósł 48,8%. Oznacza to, że sama infrastruktura nie rozwiązuje problemu edukacji cyfrowej.

- Dostęp jest wysoki, kompetencje są nierówne. Prawie każde gospodarstwo domowe ma internet, ale mniej niż połowa osób 16-74 osiąga co najmniej podstawowy poziom kompetencji cyfrowych według danych GUS.
- Młodzi są sprawni komunikacyjnie, lecz słabsi w bezpieczeństwie. Wśród osób 16-24 lata wyniki Polski w komunikacji, danych, tworzeniu treści i rozwiązywaniu problemów są wysokie, ale bezpieczeństwo cyfrowe jest istotnie niższe niż średnia UE.
- Cyberzagrożenia stają się masowe i społeczne. Według informacji gov.pl o raporcie CERT Polska w 2024 r. liczba zgłoszeń cyberzagrożeń przekroczyła 600 tys., a najczęstszym incydentem był phishing.
- Polityki publiczne idą w kierunku bezpieczeństwa i AI. Plany Ministerstwa Cyfryzacji na lata 2026-2027 obejmują cyberbezpieczeństwo, ochronę dzieci i młodzieży w internecie, walkę z dezinformacją, AI oraz kompetencje cyfrowe.
- Wniosek dla Fundacji. Najbardziej wiarygodny kierunek działań to programy łączące bezpieczeństwo cyfrowe, edukację medialną, kulturę debaty i kompetencje obywatelskie młodych ludzi.



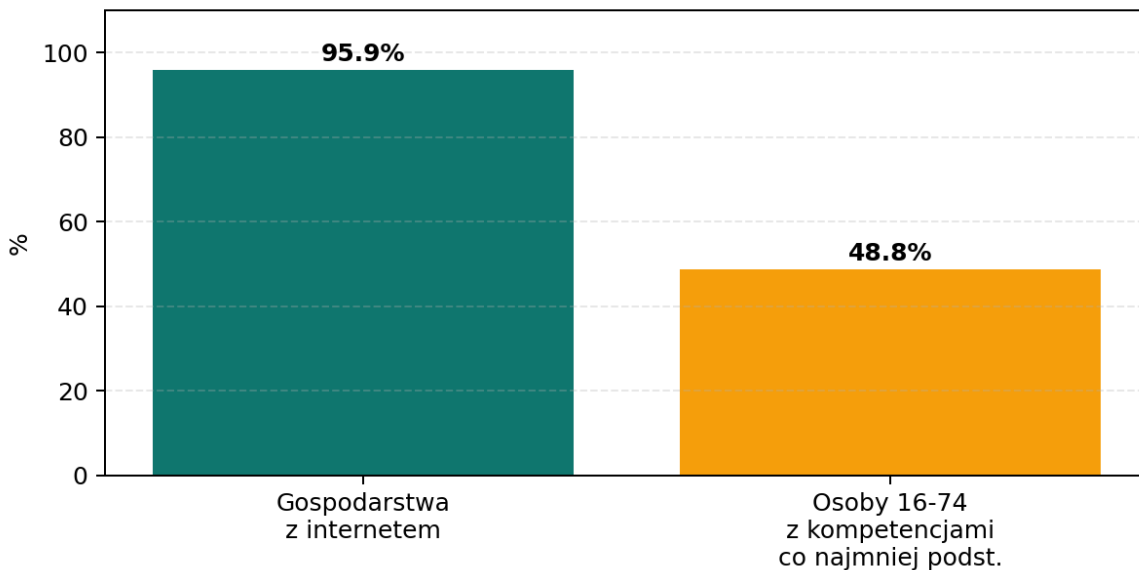
Wartości liczbowe w raporcie należy czytać jako syntetyczny wybór wskaźników publicznych, a nie jako pełne odtworzenie raportów źródłowych. Pełna lista źródeł znajduje się w aneksie.

DANE PUBLICZNE

Dostęp do technologii nie oznacza automatycznie kompetencji

Dane GUS z 2024 r. pokazują, że Polska znajduje się w fazie, w której najważniejszym zadaniem nie jest już samo doprowadzenie internetu do gospodarstw domowych, lecz rozwijanie jakościowego korzystania z narzędzi cyfrowych. Różnica między 95,9% gospodarstw z dostępem do internetu a 48,8% osób 16-74 z kompetencjami co najmniej podstawowymi wskazuje na lukę edukacyjną, społeczną i organizacyjną.

Dostęp do internetu a podstawowe kompetencje cyfrowe (GUS, 2024)



Źródło danych: GUS, Społeczeństwo informacyjne w Polsce w 2024 roku. Wykres: opracowanie własne Fundacji Obywatele Przyszłości.

Interpretacja dla działań społecznych

Wysoki poziom dostępu do internetu tworzy warunki do projektów online, ale nie gwarantuje ich skuteczności. Projekty społeczne powinny zakładać, że część odbiorców potrafi korzystać z urządzeń i aplikacji, ale nie zawsze rozumie ryzyko, mechanizmy manipulacji, zasady ochrony danych, znaczenie prywatności, konsekwencje prawne publikacji ani ograniczenia narzędzi AI.

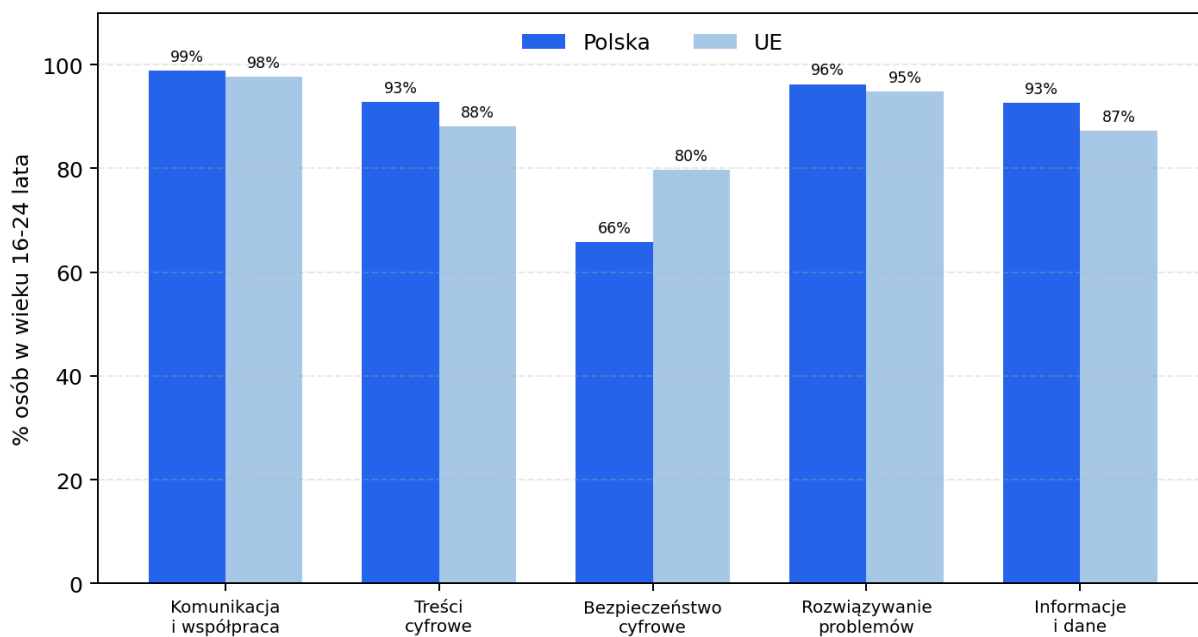
Obserwacja	Znaczenie	Implikacja dla Fundacji
Dostęp do internetu jest niemal powszechny.	Możliwe są działania ogólnopolskie prowadzone w modelu online.	Rozwijać platformy edukacyjne, wideo i bazy wiedzy dostępne bez barier geograficznych.
Kompetencje cyfrowe dorosłych pozostają ograniczone.	Technologia wymaga edukacji, nie tylko infrastruktury.	Projektować materiały prostym językiem i łączyć wiedzę techniczną z przykładami z życia.
Bezpieczeństwo cyfrowe młodych jest relatywnie słabsze.	To obszar, w którym edukacja może przynieść szybki efekt społeczny.	Budować programy o cyberhigienie, phishingu, prywatności, danych i reagowaniu na zagrożenia.

MŁODZI LUDZIE

Luka bezpieczeństwa cyfrowego w grupie 16-24 lata

Dane raportu SDG GUS pokazują, że młodzi Polacy deklarują bardzo wysokie umiejętności w obszarach komunikacji online, pracy z informacją, rozwiązywania problemów i tworzenia treści cyfrowych. Najłabszy wynik dotyczy jednak bezpieczeństwa cyfrowego: 65,85% w Polsce wobec 79,74% w Unii Europejskiej. To kluczowy wskaźnik dla projektowania działań Fundacji.

Umiejętności cyfrowe młodych osób: Polska i UE (2023)



Źródło danych: Raport SDG GUS 2025, cel 4, wskaźniki osób w wieku 16-24 lata. Wykres: opracowanie własne.

Co oznacza ta luka?

1. Nadmiar pewności

Młodzi ludzie często funkcjonują w internecie sprawnie, szybko i intensywnie. To może tworzyć przekonanie, że wysoka aktywność online jest równoznaczna z bezpieczeństwem. Dane pokazują jednak, że obszar cyberbezpieczeństwa wymaga osobnej edukacji.

2. Ryzyko socjotechniki

Największe zagrożenia nie muszą być techniczne. Oszustwa, presja czasu, fałszywe profile, wyłudzenia danych i manipulacja opierają się na zachowaniach społecznych. Dlatego edukacja musi obejmować psychologię, media i prawo.

Wniosek programowy

Fundacja powinna komunikować edukację cyfrową nie jako naukę obsługi narzędzi, ale jako kompetencję bezpiecznego życia w środowisku informacyjnym: rozpoznawania zagrożeń, oceny wiarygodności, ochrony danych, reagowania i odpowiedzialnej komunikacji.

CYBERBEZPIECZEŃSTWO

Cyberzagrożenia jako wyzwanie edukacyjne

Analiza gov.pl na podstawie raportu CERT Polska za 2024 r. wskazuje rekordowy wzrost cyberzagrożeń: ponad 600 tys. zgłoszeń, wzrost o 62% rok do roku, około 50 tys. zgłoszeń miesięcznie oraz dominację oszustw komputerowych i phishingu. To potwierdza, że cyberbezpieczeństwo nie jest tematem wyłącznie dla specjalistów IT, lecz podstawową kompetencją społeczną.

Wskaźnik publiczny	Wartość	Interpretacja edukacyjna
Zgłoszenia cyberzagrożeń do CERT Polska w 2024 r.	ponad 600 tys.	Skala zjawiska uzasadnia działania masowe, nie tylko specjalistyczne szkolenia dla wąskich grup.
Wzrost liczby zgłoszeń rok do roku	62%	Zagrożenia rosną szybciej niż zwykłe tempo adaptacji społecznej. Potrzebna jest stała edukacja.
Podejrzane wiadomości SMS	355 tys. zgłoszeń	Smishing wymaga prostych, powtarzalnych komunikatów edukacyjnych oraz nauki procedur zgłaszania.
Zablokowane złośliwe SMS-y	około 1,5 mln	Skuteczna ochrona systemowa musi być wspierana świadomością użytkowników.
Oszustwa komputerowe wśród zgłoszonych incydentów	94,7% - 97 995 incydentów	Dominacja oszustw wskazuje, że kluczowa jest odporność na manipulację i phishing.
Phishing	40 120 incydentów	To temat nadający się do scenariuszy, case studies, materiałów wideo i kampanii społecznych.

Najważniejszy trend: ataki coraz częściej wykorzystują inżynierię społeczną. Dlatego projekty edukacyjne powinny łączyć cyberhigienę z edukacją medialną, kompetencjami prawnymi i ćwiczeniem reakcji w sytuacjach presji.

REKOMENDACJE

Rekomendacje programowe dla Fundacji na lata 2026-2027

Rekomendacja	Opis działania	Proponowany rezultat
1. Program bezpiecznych kompetencji cyfrowych	Cykl lekcji, nagrań i ćwiczeń o cyberhigienie, phishingu, prywatności, danych osobowych, AI i reagowaniu na oszustwa.	Otwarte materiały edukacyjne, test wiedzy, scenariusze warsztatów.
2. Akademickie centrum bezpieczeństwa informacyjnego	Rozwój działań w środowisku studenckim: prawa studentów, procedury, reagowanie na zagrożenia, komunikacja kryzysowa.	Platforma wiedzy i seria case studies dla studentów i doktorantów.
3. Laboratorium mediów i odporności na dezinformację	Praktyczne materiały o rozpoznawaniu manipulacji, ocenie źródeł, fact-checkingu i odpowiedzialnym publikowaniu.	Baza przykładów, poradnik redakcyjny, warsztaty dla organizacji młodzieżowych.
4. Edukacja o AI dla obywateli	Moduł tłumaczący podstawy AI, ryzyka, deepfake, prywatność, prawa użytkownika i odpowiedzialne wykorzystanie narzędzi.	Mini-kurs online, webinary i poradnik dla młodych odbiorców.
5. Debaty o cyfrowej przyszłości	Cykl debat i materiałów VOD o technologii, demokracji, bezpieczeństwie, nauce i odpowiedzialności publicznej.	Nagrania, publikacje podsumowujące, pakiet tez do debat szkolnych i akademickich.

Proponowany model wskaźników

Wskaźnik produktu	Przykładowy poziom	Źródło weryfikacji
Materiały edukacyjne wideo	40-100 materiałów	Lista publikacji, statystyki platformy, archiwum VOD
Użytkownicy platformy	50 000-300 000 w zależności od skali projektu	Analityka strony, raport z zasięgów
Organizacje lub grupy odbiorców	20-50 organizacji / klas / kół / redakcji	Lista zgłoszeń, deklaracje udziału, dokumentacja wydarzeń
Wzrost wiedzy	min. 20% różnicy między pre-testem i post-testem	Test wiedzy przed i po module edukacyjnym

MODEL PROGRAMU

Proponowany projekt parasolowy: Bezpieczna Przyszłość Cyfrowa

Na podstawie przedstawionych danych Fundacja może rozwijać projekt parasolowy łączący cztery linie działań. Taki model jest czytelny dla instytucji grantowych, ponieważ posiada diagnozę, grupę docelową, kanały realizacji, mierzalne rezultaty i trwałość w postaci platformy wiedzy.

Moduł 1: Cyberhigiena młodych Phishing, smishing, hasła, prywatność, ochrona danych, bezpieczne płatności, zgłaszanie incydentów.	Moduł 2: Media i dezinformacja Ocena źródeł, fact-checking, manipulacja, algorytmy, odpowiedzialne publikowanie i reagowanie na fałszywe treści.
Moduł 3: AI i odpowiedzialność Podstawy korzystania z AI, ryzyka deepfake, prawa użytkownika, transparentność, krytyczna ocena wygenerowanych treści.	Moduł 4: Debata i obywatelskość cyfrowa Debaty, case studies, scenariusze działań, kultura rozmowy, prawa i obowiązki w cyfrowej wspólnocie.

Dlaczego ten model jest grantowo silny?

- Jest zgodny z danymi publicznymi. Odpowiada na udokumentowaną lukę między dostępem do internetu a kompetencjami oraz na słabszy wynik młodych osób w obszarze bezpieczeństwa cyfrowego.
- Jest zgodny z kierunkami polityk publicznych. Nawiązuje do cyberbezpieczeństwa, ochrony dzieci i młodzieży, AI, dezinformacji i kompetencji cyfrowych, czyli priorytetów wskazywanych w planach Ministerstwa Cyfryzacji.
- Jest skalowalny. Może działać lokalnie, regionalnie i ogólnopolsko, a jego rezultaty mogą zostać w internecie jako zasób dla kolejnych roczników odbiorców.
- Jest mierzalny. Pozwala łatwo zdefiniować wskaźniki produktu i rezultatu: liczba materiałów, odbiorców, organizacji, testów wiedzy, debat i publikacji.

ENGLISH SECTION

Executive summary

Public data from 2023-2025 show a clear mismatch between access to technology and the quality of digital competencies. In 2024, 95.9% of households in Poland had internet access, while only 48.8% of people aged 16-74 had basic or above-basic digital skills according to Statistics Poland. This means that infrastructure alone does not solve the digital education challenge.

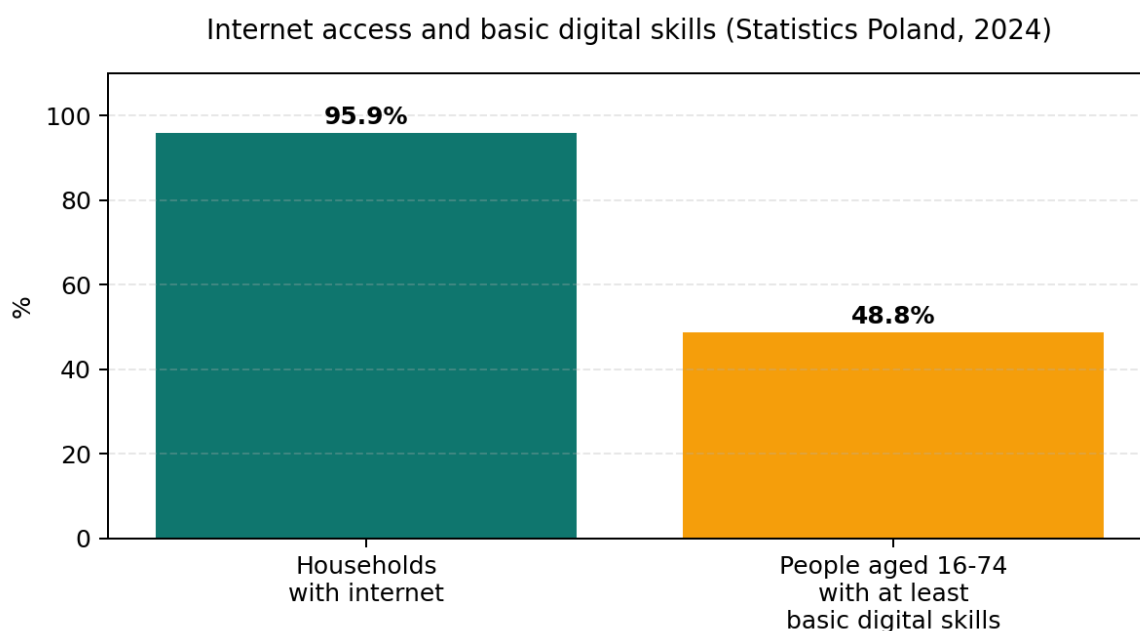
- Access is high, competencies are uneven. Almost every household has internet access, but less than half of people aged 16-74 reach at least a basic level of digital skills.
- Young people are strong in communication, but weaker in digital safety. In the 16-24 group, Poland performs well in communication, data use, content creation and problem-solving, but digital safety is significantly below the EU average.
- Cyber threats are becoming mass social risks. Government information based on the CERT Polska 2024 report points to over 600,000 cyber-threat reports and phishing as the most common incident type.
- Public policy is moving towards safety and AI. The 2026-2027 plans of the Ministry of Digital Affairs include cybersecurity, online protection of children and youth, countering disinformation, artificial intelligence and digital skills.
- Implication for the Foundation. The most credible programme direction is to combine digital safety, media literacy, civic competencies and debate culture.

95.9% households with internet access [1]	48.8% people aged 16-74 with at least basic digital skills [1]	65.85% young people 16-24 with digital safety skills [2]	600k+ cyber-threat reports to CERT Polska [3]
--	---	---	--

PUBLIC DATA

Internet access does not automatically create competence

Statistics Poland data for 2024 show that the key challenge is no longer just connecting households to the internet. The gap between 95.9% of households with internet access and 48.8% of people aged 16-74 with at least basic digital skills points to an educational and social gap.



Data source: Statistics Poland, Information Society in Poland in 2024. Chart: own elaboration.

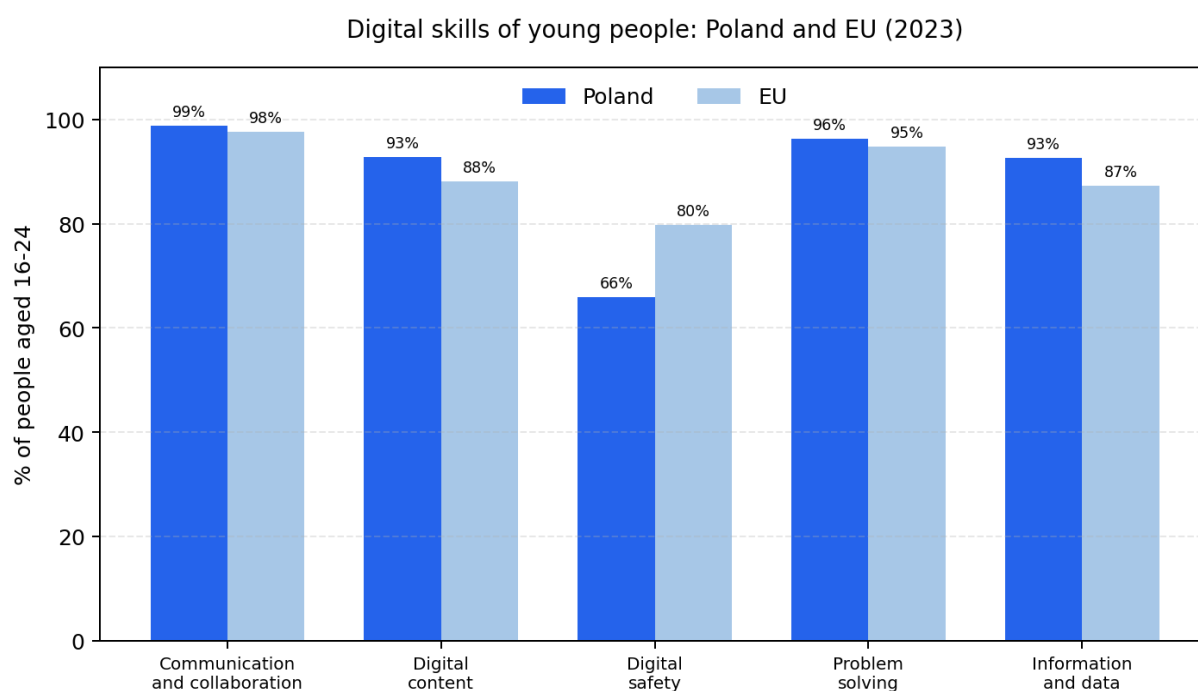
Interpretation for social projects

High internet access creates good conditions for online education projects, but it does not guarantee safe and responsible use of digital tools. Programme design should assume that many users can operate apps and platforms, but still need support in privacy, data protection, fraud prevention, AI literacy and critical source evaluation.

PUBLIC DATA

Digital skills of young people

The SDG report by Statistics Poland shows that young people in Poland have high results in online communication, data use, problem-solving and digital content creation. The weakest dimension is digital safety: 65.85% in Poland compared with 79.74% in the European Union.



Data source: Statistics Poland SDG Report 2025, Goal 4, skills of people aged 16-24. Chart: own elaboration.

Programme implication

The key opportunity is to develop education that treats digital safety as a practical life skill: recognizing threats, evaluating sources, protecting data, reacting to manipulation and using AI responsibly.

DIAGNOSIS

Cybersecurity as an educational challenge

Government analysis based on the CERT Polska 2024 report indicates a record increase in cyber threats: over 600,000 reports, a 62% year-on-year increase, approximately 50,000 reports per month, and a dominance of computer fraud and phishing. Cybersecurity should therefore be treated not only as a technical field, but as a basic social competence.

Public indicator	Value	Educational interpretation
Cyber-threat reports to CERT Polska in 2024	over 600,000	The scale of the issue justifies mass education, not only expert training for small groups.
Year-on-year increase in reports	62%	Threats are growing faster than ordinary social adaptation. Continuous education is needed.
Suspicious SMS reports	355,000	Smishing requires simple, repeatable educational messages and knowledge of reporting procedures.
Blocked malicious SMS messages	around 1.5 million	Systemic protection must be supported by user awareness.
Computer fraud among reported incidents	94.7% - 97,995 incidents	The dominance of fraud shows the importance of resilience against manipulation and phishing.
Phishing incidents	40,120	This topic is well suited for case studies, videos, workshops and social campaigns.

Programme implication

Digital education should not be framed only as tool training. It should be understood as safe life in an information environment: recognizing risks, evaluating sources, protecting data, responding to manipulation and using AI responsibly.

RECOMMENDATIONS

Programme recommendations for 2026-2027

Recommendation	Action	Expected output
1. Safe digital competencies programme	A cycle of lessons, videos and exercises on cyber hygiene, phishing, privacy, personal data, AI and fraud response.	Open educational materials, knowledge tests, workshop scenarios.
2. Academic information safety centre	Student-focused activities on rights, procedures, threat response and crisis communication.	Knowledge platform and case-study series for students and doctoral candidates.
3. Media and anti-disinformation lab	Practical content on source assessment, fact-checking, manipulation and responsible publishing.	Case database, editorial guide, workshops for youth organisations.
4. AI literacy for citizens	A module explaining AI basics, deepfake risks, privacy, user rights and responsible use of AI tools.	Online mini-course, webinars and youth-oriented guide.
5. Debates on the digital future	A series of debates and VOD materials about technology, democracy, security, science and public responsibility.	Recordings, summary publications, debate motions for schools and universities.

Umbrella project model: Safe Digital Future

The Foundation can develop an umbrella programme built around four modules: cyber hygiene, media and disinformation, AI responsibility, and digital civic debate. The model is readable for grant-making institutions because it connects diagnosis, target groups, delivery channels, measurable outputs and long-term sustainability.

Module 1: Youth cyber hygiene Phishing, smishing, passwords, privacy, data protection, secure payments and incident reporting.	Module 2: Media and disinformation Source evaluation, fact-checking, manipulation, algorithms, responsible publishing and responding to false content.
Module 3: AI and responsibility Basic AI use, deepfake risks, user rights, transparency and critical evaluation of generated content.	Module 4: Digital civic debate Debates, case studies, action scenarios, discussion culture, rights and responsibilities in digital communities.

Metodologia, ograniczenia i źródła

Metodologia. Raport przygotowano metodą desk research. Wykorzystano publicznie dostępne dane statystyczne, komunikaty i raporty instytucji publicznych. Dane zostały wybrane pod kątem projektów edukacyjnych i obywatelskich Fundacji, a następnie zinterpretowane w logice diagnozy problemu, rekomendacji oraz potencjalnych wskaźników grantowych.

Ograniczenia. Raport nie stanowi pełnego przeglądu literatury, badania reprezentatywnego ani audytu cyberbezpieczeństwa. Wskaźniki pochodzą z różnych opracowań i mogą opierać się na odmiennych metodologiach. Ich celem jest uzasadnienie kierunków działań edukacyjnych, a nie zastąpienie raportów źródłowych.

Methodology. This report was prepared using desk research based on public statistical data, government communications and public-sector reports. The data were selected for educational and civic project design and interpreted through diagnosis, recommendations and grant-oriented indicators.

Limitations. The report is not a full literature review, representative survey or cybersecurity audit. Indicators come from different publications and may use different methodologies. They support programme design and should not replace the original sources.

Źródła publiczne / Public sources

[1] Główny Urząd Statystyczny, Społeczeństwo informacyjne w Polsce w 2024 roku, informacja sygnałna, 21.10.2024
<https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2024-roku,2,14.html>

[2] Główny Urząd Statystyczny, Raport SDG 2025 - Cel 4, kompetencje cyfrowe młodzieży 16-24 lata
<https://raportsdg.stat.gov.pl/cel4.html>

[3] Gov.pl / CERT Polska, Analiza bezpieczeństwa polskiego internetu w 2024 roku, 25.04.2025
<https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku>

[4] Ministerstwo Cyfryzacji, W cyfrowym państwie żyje się lepiej - plany Ministerstwa Cyfryzacji na lata 2026-2027, 31.12.2025
<https://www.gov.pl/web/cyfryzacja/w-cyfrowym-panstwie-zyje-sie-lepiej--plany-ministerstwa-cyfryzacji-na-lata-2026-2027>

[5] PARP, Polska na drodze do cyfrowej dekady - Poland 2025 Digital Decade Country Report, 18.07.2025
<https://www.parp.gov.pl/component/content/article/88909:polska-na-drozdze-do-cyfrowej-dekady-poland-2025-digital-decade-country-report>

Nota redakcyjna

Raport zawiera opracowanie własne na podstawie publicznych danych i komunikatów. Nie jest dokumentem urzędowym ani kopią raportu GUS lub administracji rządowej. Może być wykorzystywany jako przykład kompetencji analitycznych Fundacji Obywatele Przyszłości oraz jako baza do rozwoju projektów edukacyjnych i grantowych.