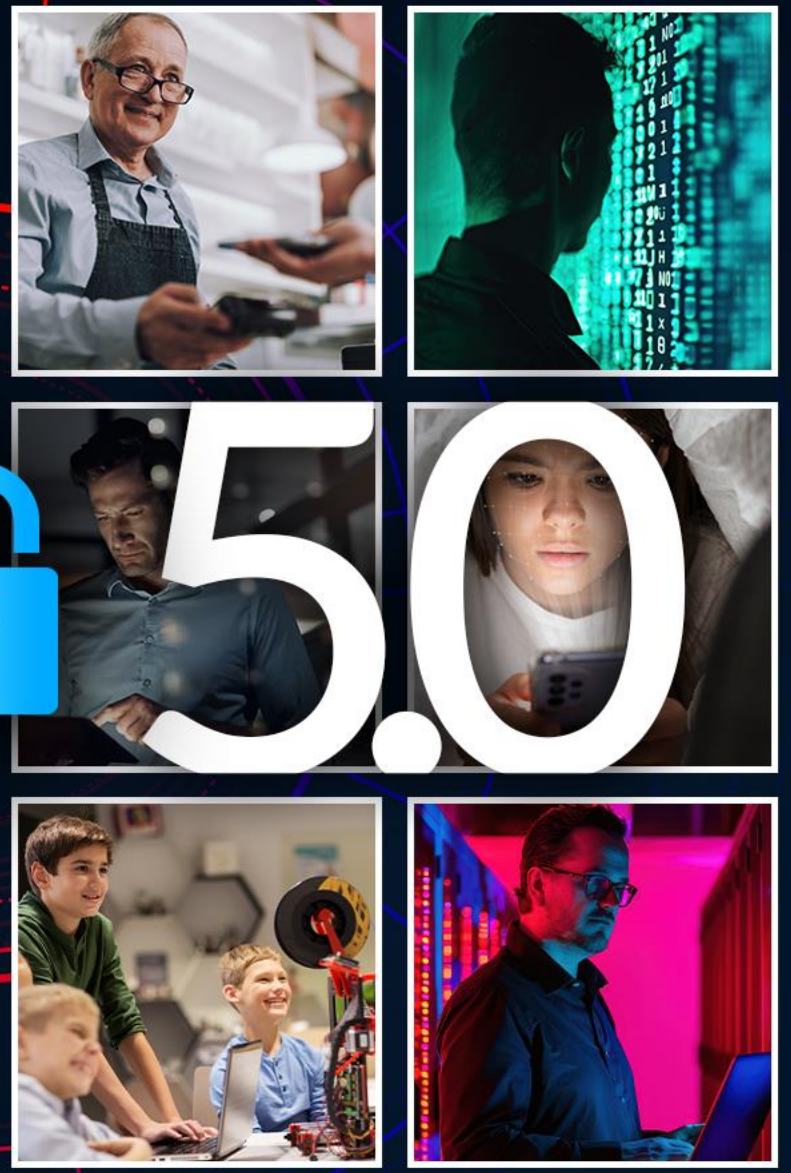
CYBERSECURITY

TECHNOLOGIA W SŁUŻBIE SPOŁECZEŃSTWU

CZY POLACY ZOSTANĄ SPOŁECZEŃSTWEM 5.0?

_2024



digitalpoland

Tytuł raportu: Technologia w służbie społeczeństwu. Czy Polacy zostaną społeczeństwem 5.0? Edycja 2024.

Edycja: 6 | Warszawa, październik 2024 r.

ISBN: 978-83-971647-3-4

Wydawca: Fundacja digitalpoland

digitalpoland

Stępińska 22/30, 00-739, Warszawa, Polska
info@digitalpoland.org | digitalpoland.org | digitalfestival.pl | digitalshapers.pl | digitalars.pl | aipoland.org | eaiforum.org

Finansowanie: Publikacja sfinansowana ze środków pozyskanych od Partnerów raportu przeznaczonych na edukację społeczeństwa oraz statutowych.

Partnerzy raportu: 100 1924 - 2024 BGK POLSKI BANK ROZWOJU; GfK An NIQ Company

Redakcja: Piotr Mieczkowski

Podziękowania: Fundacja Digital Poland pragnie podziękować Partnerom raportu i Fundatorom, dzięki którym może realizować swoją misję. Więcej informacji na digitalpoland.org/kto

Projekt, DTP: Krzysztof Waloszczyk | So! Creative House | www.socreativehouse.pl

SPIS TREŚCI

PRZEDMOWA

Piotr Mieczkowski

Dyrektor zarządzający, Członek zarządu fundacji Digital Poland, Wiceprezes zarządu European AI Forum, Ekspert KIGEiT, Członek grup roboczych przy Ministerstwie Cyfryzacji

W epoce cyfrowej rewolucji, gdy nasze życie coraz bardziej przenosi się do sfery online, kwestia cyberbezpieczeństwa nabiera bezprecedensowego znaczenia. Raport, który oddajemy w Państwa ręce, stanowi kompleksowe spojrzenie na stan cyberbezpieczeństwa Polaków – tak istotnego dla społeczeństwa 5.0. Wyniki naszych badań malują obraz społeczeństwa, które stoi w obliczu poważnych wyzwań związanych z bezpieczeństwem w sieci.

Żyjemy w czasach, w których geopolityczne napięcia przekładają się na zwiększoną liczbę ataków w cyberprzestrzeni, a jednocześnie coraz więcej aspektów naszego codziennego życia realizujemy za pośrednictwem internetu. W tym kontekście, umiejętność bezpiecznego poruszania się w świecie online staje się kluczową kompetencją XXI wieku. Niestety, jak wykazują nasze badania, wielu Polaków wciąż nie posiada wystarczającej wiedzy i umiejętności w tym zakresie.

Alarmujący jest fakt, że co trzeci Polak ma niewielką wiedzę o cyberbezpieczeństwie, a aż 45% nie zdało naszego testu na temat phishingu – jednego z najpowszechniejszych zagrożeń w sieci. To jasny sygnał, że edukacja w zakresie bezpieczeństwa cyfrowego powinna stać się priorytetem zarówno dla instytucji państwowych, jak i sektora prywatnego.

Aż 65% Polaków deklaruje obawy o swoje bezpieczeństwo w internecie. Co więcej, połowa z tych osób ogranicza swoją aktywność online z powodu lęku przed zagrożeniami. To zjawisko, które można określić mianem cyfrowego wycofania, stanowi poważne wyzwanie dla rozwoju gospodarki cyfrowej i pełnego wykorzystania potencjału, jaki niesie ze sobą era informacji. Obawy związane z cyberbezpieczeństwem hamują rozwój cyfryzacji w Polsce – wielu Polaków z powodu leków boi się np. robić zakupy w internecie czy korzystać z zaawansowanych usług cyfrowych.

Szczególnie niepokojące są statystyki dotyczące bezpośrednich doświadczeń Polaków z cyberprzestępczością. Aż 36% respondentów padło ofiarą cyberataków lub oszustw internetowych w ciągu ostatniego roku. Jednocześnie warto zauważyć, że ponad połowa Polaków doświadczyła próby oszustwa internetowego (scamu), co świadczy o skali tego zjawiska i konieczności podjęcia zdecydowanych działań w celu jego ograniczenia. Co więcej, 80% Polaków uważa, że w perspektywie kolejnych pięciu lat skala tego zjawiska wzrośnie. Raport ujawnia również rosnące przekonanie społeczeństwa o konieczności wprowadzenia regulacji prawnych w obszarze cyberbezpieczeństwa. Aż 73% Polaków popiera pomysł wprowadzenia kar dla dużych platform internetowych za brak lub zbyt powolną reakcję na oszustwa. To jasny sygnał dla ustawodawców, że społeczeństwo oczekuje bardziej zdecydowanych działań w walce z cyberprzestępczością.

Szczególną uwagę należy zwrócić na kwestię ochrony dzieci w internecie. 56% Polaków uważa, że obecne prawo nie chroni wystarczająco najmłodszych przed nieodpowiednimi treściami online. Co więcej, 75% respondentów opowiada się za tym, aby zakazy obowiązujące w świecie rzeczywistym były równie rygorystycznie egzekwowane w internecie. Polakom brakuje przy tym wiedzy – jedynie 3 na 10 poprawnie wskazało na wymagany minimalny wiek uprawniający do założenia konta w mediach społecznościowych. Pewnie w związku z tym aż 73% Polaków popiera wprowadzenie weryfikacji wieku w sieci dla treści dla dorosłych. Te dane powinny skłonić do refleksji i działania zarówno rodziców, jak i decydentów odpowiedzialnych za tworzenie ram prawnych chroniących dzieci w sieci.

Niepokojącym zjawiskiem jest również wszechobecność mowy nienawiści w internecie. Co trzeci Polak osobiście doświadczył tego problemu, a 73% uważa, że w sieci jest zbyt dużo nienawistnych treści. To kolejny obszar, w którym społeczeństwo oczekuje konkretnych działań prawnych i edukacyjnych. Jednym z rozwiązań może być wprowadzenie do porządku prawnego definicji mowy nienawiści ale również tzw. ślepego pozwu.

Warto podkreślić, że mimo tych wszystkich wyzwań Polacy deklarują znaczenie pochodzenia rozwiązań technologicznych. Połowa respondentów deklaruje, że przy wyborze narzędzi do ochrony online ważny jest dla nich kraj pochodzenia dostawcy, a 70% z nich preferuje rozwiązania polskie. To dobry prognostyk dla rozwoju rodzimego sektora cyberbezpieczeństwa. Co ciekawe, liderzy cyberbezpieczeństwa, tacy jak Izrael czy Korea Południowa, cieszą się podobnym zaufaniem jak Chiny, Indie czy Rosja.

Jednakże mimo rosnącej świadomości zagrożeń wciąż istnieje ogromna luka w edukacji z zakresu cyberbezpieczeństwa. Zaledwie 10% społeczeństwa brało udział w kampaniach zwiększających wiedzę na ten temat. To jednoznacznie wskazuje na potrzebę intensyfikacji działań edukacyjnych i informacyjnych.

Przedstawione w raporcie dane powinny stanowić impuls do działania dla wszystkich zainteresowanych stron: rządu, sektora prywatnego, organizacji pozarządowych i samych obywateli. Konieczne jest podjęcie skoordynowanych wysiłków w celu podniesienia poziomu cyberbezpieczeństwa w Polsce. Obejmuje to zarówno intensyfikację działań edukacyjnych, jak i wprowadzenie odpowiednich regulacji prawnych, które będą chronić użytkowników internetu, a jednocześnie nie hamować rozwoju gospodarki cyfrowej. Mamy nadzieję, że niniejszy raport przyczyni się do pogłębienia debaty na temat cyberbezpieczeństwa w Polsce i stanie się katalizatorem konkretnych działań.

Anna Węgrzynowicz

Biuro Zaangażowania Społecznego, Projekt Digital Sustainability (DigSus), Bank Gospodarstwa Krajowego

Technologia odgrywa coraz większą rolę w codziennym życiu, zmieniając sposób, w jaki funkcjonujemy, pracujemy, komunikujemy się. Przez postęp cyfryzacji pojawia się coraz większe zapotrzebowanie na analizę wpływu technologii na społeczeństwo oraz identyfikację, w jaki sposób ma ona służyć jego dobrobytowi. Ten raport skupia się na roli technologii w służbie społeczeństwu, wskazując różnorodne obszary, w których może ona przyczynić się do poprawy warunków życia, rozwoju gospodarczego i tworzenia społeczeństwa opartego na innowacjach i równości dostępu do korzyści wynikających z technologicznego postępu. Pokazuje na konkretnych przykładach związanych z ochroną zdrowia, energią, cyfryzacją usług publicznych czy zrównoważonym rozwojem potencjał technologiczny w transformacji społeczeństwa. Jest też inspiracją do dalszych działań, które pozwalają budować lepszy i bardziej zrównoważony świat. Integracja cyfrowego i zrównoważonego rozwoju tzw. Koncepcja „twin transition" stanowi kluczowe wyzwanie we współczesnym świecie i innowacyjne podejście do rozwoju miast i gospodarek.

Z perspektywy Banku Gospodarstwa Krajowego ważne jest finansowe stymulowanie rynku nowych technologii, zgodnie z zasadami zrównoważonego rozwoju. Dotyczy to zwłaszcza sektorów ochrony zdrowia i energetyki. BGK jest dystrybutorem środków z Krajowego Planu Odbudowy na inwestycje związane z transformacją cyfrową, energetyczną oraz zieloną transformacją miast, co ma istotny wpływ na gospodarkę w tych właśnie obszarach.

Raport pokazuje, że mężczyźni częściej korzystają z nowych technologii niż kobiety, co wskazuje na potrzebę wsparcia inicjatyw, które promują cyfryzację wśród kobiet. Ważne jest również wsparcie osób z mniejszych miejscowości oraz dbałość o minimalizowanie negatywnego wpływu cyfryzacji na społeczeństwo. Projekt Digital Sustainability (DigSus) jest odpowiedzią na zjawiska społeczne, które wiążą się z nowymi technologiami takim, jak np. rozwój AI. To z jednej strony codzienne funkcjonowanie pracowników, z drugiej – kryzys zdrowia psychicznego.

Jednym z głównych wyzwań przyszłości, na którym jako społeczeństwo powinniśmy się skoncentrować, jest rozwój edukacji cyfrowej. Tylko to pozwoli nam w pełni wykorzystać możliwości, jakie niesie ze sobą transformacja cyfrowa. Musimy zrozumieć rolę technologii oraz jej świadome i umiejętne wykorzystanie w kontekście rozwoju osobistego i zawodowego.

Współpraca między sektorem publicznym, prywatnym oraz społeczeństwem jest niezbędna, aby opracowywać nowe technologie wspierające poprawę jakości życia i efektywność działania różnych sektorów gospodarki. Wyniki raportu wskazują, że Polacy coraz chętniej korzystają z nowoczesnych technologii, zwłaszcza w obszarach ochrony zdrowia, energii oraz cyfryzacji usług publicznych. Rośnie także świadomość ekologiczna oraz potrzeba automatyzacji i poprawy efektywności energetycznej.

Jednocześnie musimy zadbać o zapewnienie powszechnego dostępu do Internetu i narzędzi cyfrowych, aby zapobiegać wykluczeniu cyfrowemu. Szczególną uwagę należy poświęcić osobom w wieku 50+, które nadal są aktywne zawodowo, pomóc im rozwijać swoje umiejętności w obszarze cyfryzacji. Ważne jest, aby dostosować edukację do potrzeb tej grupy wiekowej, zapewnić dostęp do odpowiednich szkoleń i kursów. Dbałość o „leave no one behind" to kluczowy element budowy społeczeństwa cyfrowego, w którym wszyscy mają możliwość korzystać z rozwoju technologicznego.

Technologia ułatwia utrzymywanie kontaktu z bliskimi, zdobywanie nowej wiedzy i umiejętności, a także zwiększa świadomość zagrożeń. Ważną kwestią pozostaje bezpieczeństwo w cyberprzestrzeni, w tym ochrona danych osobowych. Czynniki sprzyjające cyberprzestępczości takie jak nieostrożność potencjalnych ofiar, nieodpowiednie zabezpieczenia czy też brak wiedzy – zwiększają prawdopodobieństwo skutecznego przeprowadzenia ataku. Umiejętność rozpoznania fałszywego maila, lub też zasada ograniczonego zaufania powinny towarzyszyć nam codziennie. Świat cyfrowy rozwija się dynamicznie, technologia jest integralną częścią naszej codzienności. Dlatego też budujmy naszą świadomość i edukujmy naszych znajomych i rodzinę w tym aspekcie, aby utrudnić cyberprzestępcom osiągnięcie celu.

Jest jeszcze jedno niebezpieczeństwo. To cyberprzemoc i hejt. Aby wygrać z agresją w sieci, niezbędne jest, aby uwzględniać aspekty etyczne i odpowiedzialne korzystanie z technologii cyfrowych. Cyberprzemoc i hejt w sieci stanowią poważne zagrożenia, sprzyjające agresywnym zachowaniom. Niezbędne jest przeciwdziałanie takim zjawiskom poprzez promowanie kultury szacunku i empatii w przestrzeni cyfrowej.

Technologia zmienia nasz świat, a jej odpowiedzialne i etyczne wykorzystanie ma ważne znaczenie dla budowania świadomego społeczeństwa. Mamy nadzieję, że ten raport to nie tylko solidna dawka wiedzy, lecz także inspiracja do zmian.

Życzę owocnej lektury.

JAK CZYTAĆ RAPORT

Raport przedstawia wyniki dwóch reprezentatywnych badań polskiego społeczeństwa

Pierwsze badanie dotyczy technologii w służbie społeczeństwu czyli próbie odpowiedzi na pytanie czy Polacy staną się społeczeństwem 5.0.

Zbadaliśmy zatem świadomości polskiego społeczeństwa co do strategicznych wyzwań, przed jakimi stoi nasz kraj czy ogólnego nastawienia do technologii. W raporcie przedstawiliśmy technologiczny profil społeczeństwa jak i informacje o gotowości Poleki Polaków do skorzystania z konkretnych rozwiązań, które pozwalają rozwiązać część problemów, z jakimi boryka się Polska. Pierwszy rozdział prezentuje zatem gotowość polskiego społeczeństwa do stania się społeczeństwem 5.0, w którym nowe technologie, takie jak AI oraz integracja świata cyfrowego z rzeczywistym, odgrywają kluczową rolę. Na kolejnych stronach pierwszego rozdziału zaprezentowano wyniki 6. edycji reprezentatywnego badania społeczeństwa wykonanego metodą CAWI. W związku ze zmianą metodologii badania raport przedstawia ranking wyzwań, nastawienia do technologii czy chęć skorzystania z technologii w porównaniu tylko danych z roku ubiegłego. W pytaniach stosowano pięciostopniową skalę Likerta, a skrajne wyniki, np. „zdecydowanie tak" i „raczej tak" oraz „zdecydowanie nie" i „raczej nie", zsumowano. W raporcie zaprezentowano również wyniki z podziałem na standardowe segmenty takie jak płeć, wiek, lokalizacja czy wykształcenie. Część danych może nie sumować się do 100% z racji stosowanych zaokrągleń.

RANKING	Różnica w rankingu vs 2023
1	+4 ↑
2	-1 ↓
3	-1 ↓
4	0 =

Drugie badanie dotyczy stanu cyberbezpieczeństwa w Polsce oczami Polaków.

W fundacji co roku podejmujemy się badania na inny, dodatkowy temat. W ubiegłych latach sprawdziliśmy opinię Polaków na temat kompetencji cyfrowych, ESG/SDG, a ostatnio na temat sztucznej inteligencji (AI). Obecnie, z uwagi na rosnące napięcia geopolityczne, rosnącą skalę ataków na świecie i wstępną hipotezę o negatywnym wpływie obaw Polaków o swoje bezpieczeństwo na aktywność w sieci postanowiliśmy prze-prowadzić najbardziej kompleksowe badanie cyberbezpieczeństwa w Polsce z punktu widzenia konsumenta, obywatela. Z uwagi też na ważne sprawy społeczne takie jak rosnąca skala mowy nienawiści czy niewystarczająca ochrona dzieci w internecie podjęliśmy decyzję o zbadaniu opinii Polaków i w tych kwestiach. W naszych pracach zawsze kierujemy się analizą danych i wskazywaniem rekomendacji na bazie faktów stąd swoim badaniem pragniemy też wesprzeć debatę publiczną w sprawie zwiększenia poziomu cyberbezpieczeństwa w Polsce. Przy tworzeniu kwestionariusza skorzystaliśmy z najlepszych światowych praktyk w tej tematyce oraz konsultowaliśmy się z ekspertami.

By łatwiej zrozumieć raport, przy większości z odpowiedzi można znaleźć szereg ikon dokładnie wskazujących na konkretny segment.

PODSUMOWANIE ZARZĄDCZE

1. SPOŁECZEŃSTWO 5.0, CZYLI ZRÓWNOWAŻONEGO ROZWOJU DZIĘKI TECHNOLOGII

1.1. Strategiczne wyzwania stojące przed Polską

W 6. edycji badania poszukiwano odpowiedzi na pięćdziesiąt głównych wyzwań strategicznych, które stoją przed Polską. Do najważniejszych z nich można zaliczyć: zbyt długie kolejki do lekarza i szpitala (81%), utrzymująca się drożyzna (80%), starzenie się społeczeństwa (78%), duża biurokracja (77%) oraz ograniczony dostęp do mieszkań dla młodych Polaków (75%). W czołówce znajdują się też wyzwania dotyczące polaryzacji społeczeństwa i nierówności społeczno-finansowych, z obszaru zdrowia, jakości instytucji państwowych i sprawnego państwa (np. 70% wskazuje na brak obiektywnych i niezależnych od władzy urzędników, 74%, brak przełożenia podatków na jakość usług publicznych) oraz ochrony środowiska i zmian klimatu. Równie ważne są problemy z rosnącą dezinformacją (67%), rozpadem więzi społecznych (68%), brakiem przemyślanej i odpowiedzialnej polityki imigracyjnej (65%). Nadal istotna jest sprawa niedokończonej transformacji energetycznej. Wielu z nas ciągle uważa, że jesteśmy zbyt uzależnieni od węgla i za mało korzystamy z energii odnawialnej (ponad 64%). W pierwszej dwudziestce wyzwań znalazły się jedynie dwa wyzwania związane wprost z cyfryzacją – nieinwestowanie w kwalifikacje pracowników (69%) i wspomniany brak edukacji medialnej, przez co społeczeństwo jest podatne na dezinformację (67%).

Trochę mniej istotne (ok. 63–55%) dla Polaków są wyzwania dotyczące braku innowacyjności przemysłu i polskich firm, braku pełnego upowszechnienia płatności bezgotówkowych na terenie całego kraju, zbyt niskiego wykorzystania nowych technologii czy niskiej produkcji półprzewodników. Wyzwania związane z innowacyjnością znalazły się w trzeciej i czwartej dziesiątce rankingu, a np. kwestia uzależnienia od bigtech na 33. miejscu. W ocenie Polaków nie jesteśmy też celem zbyt wielu cyberataków w internecie (42. miejsce). Większość wyzwań związanych z cyfryzacją znajduje się dopiero w czwartej i piątej dziesiątce rankingu.

Strategiczne wyzwania związane z realizacją Cyfrowej Dekady 2030 są natomiast najmniej istotne dla polskiego społeczeństwa i plasują się w ostatniej dziesiątce ocenianych wyzwań. Nie spędzają one snu z powiek Polaków. Na brak możliwości załatwiania spraw przez internet, słaby dostęp do szybkiego internetu czy zbyt niski poziom kompetencji Polaków wskazuje ok. 49%. Z kolei zbyt mała liczba informatyków jest istotna dla jedynie 38% z nas.

W tegorocznym badaniu najbardziej wzrosło zaniepokojenie nierównościami społeczno-finansowymi (obecnie na 11. miejscu w rankingu i jest to przesunięcie do góry o 11 miejsc) oraz to, że pracodawcy nie inwestują wystarczająco w rozwój i kwalifikacje swoich pracowników (obecnie na 16. miejscu w rankingu i jest to przesunięcie do góry o 11 miejsc).

Najbardziej zmalały natomiast obawy o to, że media są podporządkowane celom politycznym i że w Polsce nie ma rządów prawa (spadek w rankingu aż o 19 miejsc, odpowiednio na 25. i 48. miejsce). Ponadto bardzo zmniejszyły się obawy o możliwość bankructwa systemu emerytalnego (obecnie na 27. miejscu w rankingu i jest to spadek o 13 miejsc) oraz obawy, że w Polsce nie są chronione podstawowe wolności jednostki (obecnie na 45. miejscu w rankingu i jest to spadek o 12 miejsc).

1.2.

Nastawienie do nowych technologii oraz technologiczny profil Polaków

Większość z nas pozytywnie postrzega technologię – jako dającą nowe możliwości. Pozytywnie oceniamy umiejętności cyfrowe, uważając je za klucz do lepszej pracy (72%) i ułatwienie codziennego życia (73%). Nasze społeczeństwo chętnie korzysta z technologii (60%), a internet jest postrzegany jako narzędzie niwelujące różnice między obszarami miejskimi i wiejskimi (69%). Cieszy również fakt, że korzystanie z cyfryzacji i nowych technologii jest dla niewielu z nas zbyt skomplikowane (30%).

Jednocześnie Polacy dostrzegają negatywne strony nowych technologii, łącząc postępującą cyfryzację z rozpadem więzi społecznych, mniejszą otwartością na rozmowy z innymi (71%). Dla niecałych 30% z nas korzystanie z technologii prowadzi do ciężkich chorób. W naszej ocenie część obaw dotyczących negatywnego wpływu technologii na nasze zdrowie może wynikać z szerzącej się dezinformacji na temat rzekomo masowo palących się aut elektrycznych, zabójczych sieci 5G czy sztucznej inteligencji. Ubiegłoroczna burza w mediach dotycząca generatywnej AI oraz wejście AI do mainstreamu sprawiło, że pesymistyczne nastawienie do technologii, robotyki i AI utrzymuje się na poziomie z ubiegłego roku (około 55%). Jedynie 23% Polaków uważa, że nowe technologie są zbędne.

Mężczyźni częściej deklarowali chęć sięgania po nowinki technologiczne (68 vs 53%), kobiety z kolei – że nowe technologie sprawiają, że ludzie zbyt rzadko ze sobą rozmawiają (75 vs 66%), technologia tworzy sztuczny świat (59 vs 53%) czy że rozwój robotyki i sztucznej inteligencji jest zagrożeniem dla miejsc pracy (57 vs 51%). Najmłodsza grupa Polaków częściej przyznaje natomiast, że cyfryzacja i nowe technologie są zbędne (33 vs 10%) oraz że korzystanie z nowych technologii prowadzi do ciężkich chorób (33 vs 13%). Powyższe wyniki przeczą popularnym tezom, jakoby to młodzi ludzi widzieli większe szanse w nowych technologiach czy starsi bardziej obawiali się ciężkich chorób. Miejsce zamieszkania nie jest znaczącym wyróżnikiem w zakresie nastawienia do nowych technologii i cyfryzacji. Wykształcenie jest nadal najważniejszym czynnikiem, który mocno różnicuje nastawienie do nowych technologii i cyfryzacji. Różnica w nastawieniu potrafi sięgać blisko 40 punktów procentowych.

Polacy z wyższym wykształceniem znacząco częściej niż posiadający podstawowe wykształcenie przyznają, że technologia ułatwia im codzienne życie (79 vs 41%), chętnie sięgają po nowinki technologiczne (66 vs 29%), umiejętności cyfrowe zwiększają szansę na znalezienie lepszej pracy (76 vs 55%). Osoby z podstawowym wykształceniem częściej zgadzają się, że rozwój robotyki i AI jest zagrożeniem dla miejsc pracy (63 vs 50%), cyfryzacja jest zbędna (29 vs 19%), a technologia tworzy sztuczny świat (58 vs 51%).

Z punktu widzenia segmentacji i technologicznych profili Polaków to blisko 65% Polaków jest nastawionych pozytywnie do nowych technologii. Można ich ująć jako entuzjastów (16%), realistów (22%) czy pragmatyków (26%). Największymi entuzjastami technologii są częściej mężczyźni, trochę częściej osoby w wieku 30-49 i 60-75 lat, częściej z wykształceniem średnim lub wyższym, częściej z dużych miast, częściej w dobrej sytuacji ekonomicznej, częściej codziennie korzystający z internetu. Z kolei 17% z nas deklaruje się jako zdystansowani, a 19% jako ostrożni wobec cyfryzacji. Najbardziej ostrożne są najczęściej kobiety, częściej w wieku 60–75 lat, częściej z podstawowym wykształceniem, częściej o słabej sytuacji ekonomicznej, trochę częściej mieszkające w miasteczkach.

1.3.

Chęć korzystania z nowych technologii odpowiadających na strategiczne wyzwania stojące przed Polską

Podobnie jak w ubiegłym roku, tak i w 2024, recykling i produkty ekologiczne nadal cieszą się największą popularnością wśród Polaków (blisko 70–60%), co świadczy o rosnącej świadomości ekologicznej i gotowości do wsparcia gospodarki obiegu zamkniętego. Z chęcią też skorzystamy ze źródeł odnawialnych, co powinno ułatwić transformację energetyczną.

Cyfryzacja jako taka zyskała poparcie nieco ponad 50% badanych (np. załatwianie spraw przez internet czy głosowanie do Sejmu i Senatu RP).

Najlepiej ocenianym narzędziem bazującym na sztucznej inteligencji (AI) jest indywidualny asystent, wspierający w zadaniach zawodowych i edukacyjnych, co przyczynia się do wzrostu efektywności i zapewnia dodatkowy czas wolny (51%). Zaawansowane użycia AI, takie jak autonomiczne pojazdy czy operacje chirurgiczne wykonane przez roboty, nadal mają jednak tylko około 30% akceptacji. Zatem 2/3 Polaków nie jest gotowych np. wsiąść do pociągu bez maszynisty, sterowanego przez AI. Czterech na 10 Polaków chce skorzystać z innowacyjnych metod płatności dokonywanych za pomocą odcisku palca czy twarzy. Co czwarty Polak jest otwarty na kryptowaluty.

W tegorocznym badaniu najbardziej wzrosło zainteresowanie dostępnością antybiotyków i leków przez internet (obecnie na 6. miejscu w rankingu i jest to przesunięcie do góry o 10 miejsc) oraz możliwość załatwiania wszystkich spraw urzędowych i administracyjnych cyfrowo i całkowicie zrezygnowanie z tradycyjnej oraz papierowej formy komunikacji (obecnie na 8. miejscu w rankingu i jest to przesunięcie do góry o 5 miejsc).

Najmocniej natomiast spadła akceptacja wymiany organów (np. wątroba) na nowe, które zostały wydrukowane lub wyhodowane (obecnie na 18. miejscu w rankingu i jest to spadek o 7 miejsc). Zmalała również akceptacja dla prądu z elektrowni atomowej wybudowanej w województwie respondenta (obecnie na 13. miejscu w rankingu i jest to spadek o 6 miejsc) oraz chęć korzystania z asystenta AI (program komputerowy) w pracy, nauce (obecnie na 14. miejscu w rankingu i jest to spadek o 6 miejsc).

Mężczyźni bardziej niż kobiety są otwarci na skorzystanie z nowoczesnych rozwiązań. Najmłodsi Polacy (w wieku 18–24) znacząco częściej niż najstarsi (w wieku 60+) są skłonni skorzystać z nowych technologii, jak otrzymanie wynagrodzenia w kryptowalucie (36 vs 9%), zastępowanie produktów mięsnych przez zamienniki roślinne i owady (41 vs 18%), podróżowanie autonomicznym autobusem (38 vs 21%), korzystanie ze sklepu bez obsługi (61 vs 45%), dostarczenie zakupów i przesyłek przez roboty. Z kolei najstarsze osoby znacząco częściej niż najmłodsze są otwarte na rozwiązania ekologiczne, jak produkty uzyskane z recyklingu (77 vs 57%), panele słoneczne na dachach domów do produkcji czystego prądu (59 vs 47%). Mieszkańcy największych miast (powyżej 500 tys. mieszkańców) częściej niż mieszkańcy wsi są bardziej otwarci na głosowanie w wyborach przez internet (67 vs 47%), panele słoneczne na dachach domów do produkcji czystego prądu (75 vs 58%), dostępność przez internet antybiotyków i leków na receptę (66 vs 51%). Wykształcenie jest najważniejszym czynnikiem, który mocno różnicuje chęć skorzystania z nowych technologii – różnice w nastawieniu wynoszą nawet 33 punkty procentowe. Szczególnie jest to widoczne w odniesieniu do głosowania w wyborach przez internet (63 vs 30%), korzystania z indywidualnego programu stworzonego przez AI w celu analizy braków w umiejętnościach cyfrowych (54 vs 24%), wymiany organów (np. wątroba) na nowe, które zostały wydrukowane lub wyhodowane (56 vs 27%), używania produktów z recyklingu (79 vs 50%).

2. CYBERBEZPIECZEŃSTWO OCZAMI POLAKÓW 2024

2.1.

Jaką mamy wiedzę na temat cyberbezpieczeństwa?

Co trzeci Polak ma małą wiedzę o cyberbezpieczeństwie. To częściej kobiety (41 vs 25%), osoby starsze (48 vs 15%), mieszkające na wsi (39 vs 19%) oraz posiadające podstawowe wykształcenie (43 vs 26%). 39% Polaków wykazuje umiarkowaną wiedzę na temat cyberbezpieczeństwa, a 28% – dużą.

Aż 45% Polaków nie zdało naszego testu na temat phishingu. Częściej były to osoby młodsze (58 vs 37%), z wykształceniem podstawowym (55 vs 46%). Pocieszający jest fakt, że 2 na 3 Polaków chce pogłębić swoją wiedzę z zakresu cyberbezpieczeństwa. To częściej osoby starsze (71 vs 58%) i z wyższym wykształceniem (71 vs 53%).

Trzech na 10 Polaków nie wie, jak postąpić w przypadku cyberataku lub incydentu. Co piąty czuje się zagubiony. Tylko ok. 25% zna procesy i wie, do kogo się zgłosić.

W razie cyberataku, oszustwa lub incydentu cyberbezpieczeństwa Polacy udadzą się na policję lub do innych lokalnych organów ścigania(41%), instytucji finansowej (np. w przypadku naruszenia informacji finansowych lub kont – 38%). Jedynie 1 na 4 wybrałby służby państwowe, z kolei 20% skorzystałoby z pomocy rodziny lub znajomego. Co dwudziesty Polak nic by nie zrobił w przypadku cyberataku czy oszustwa. Największe różnice w zachowaniu można zaobserwować w podziale na rodzaj wykształcenia. Polacy z wyższym wykształceniem znacząco częściej niż posiadający podstawowe wykształcenie udaliby się na policję lub do innych lokalnych organów ścigania (46 vs 26%), znajomych z wiedzą IT (27 vs 11%), służb państwowych takich jak CSIRT (29 vs 17%) czy działu IT pracodawcy (22 vs 12%). Z kolei osoby z wykształceniem podstawowym znacząco częściej skontaktowałyby się z dostawcą usług internetowych (35 vs 18%) czy profesjonalną firmą świadczącą usługi z zakresu cyberbezpieczeństwa (22 vs 8%).

Co czwarty Polak ma zbyt dużo kont w internecie do zakupów, logowania, płatności czy mediów społecznościowych lub ma ich więcej niż jedenaście. Częściej są to osoby młode (40 vs 14%), z dużych miast (35 vs 24%) i z wyższym wykształceniem (37 vs 21%). 14% Polaków nie kontroluje już liczby kont, którymi się posługuje, co ułatwia cyberataki.

2.2.

Czy czujemy się bezpiecznie w sieci i czy ma to wpływ na naszą aktywność?

Aż 65% Polaków martwi się o swoje bezpieczeństwo w internecie. Są to częściej kobiety (69 vs 61%), osoby starsze (76 vs 55%). Co druga z osób martwiących się o swoje bezpieczeństwo w wyniku lęków ogranicza aktywność w internecie. Oznacza to, że blisko 32% Polaków boi się podejmować pewne aktywności w sieci z uwagi na możliwość cyberataku, incydentu lub innego zagrożenia.

Największe obawy związane z korzystaniem z internetu dotyczą kradzieży tożsamości lub przejęcia konta (61%), zainstalowania złośliwego oprogramowania na urządzeniu elektronicznym (55%) oraz wyłudzenia bądź kradzieży pieniędzy (54%). Dezinformacji obawiało się 30%, a hejtu 22% Polaków. Tylko 4% deklaruje, że nie obawia się niczego podczas korzystania z internetu. Kobiety częściej niż mężczyźni boją się o różnego rodzaju aktywności. Największe różnice na korzyść kobiet zaobserwowano dla obaw związanych z użyciem wizerunku do stworzenia deepfake (34 vs 22%), wyłudzeniem czy utratą swoich danych osobowych (50 vs 40%). Osoby młodsze zdecydowanie częściej obawiały się mowy nienawiści, naruszenia własnej godności osobistej, ośmieszenia czy zastraszenia (32 vs 17%), deepfake i fałszywych wiadomości (18 vs 11%) oraz dezinformacji (40 vs 35%). Mieszkańcy największych miast częściej niż mieszkańcy wsi obawiają się awarii usług i aplikacji w internecie, kiedy będą ich potrzebować (30 vs 23%). Z kolei mieszkańcy wsi obawiają się użycia ich wizerunku do stworzenia deepfake z wykorzystaniem sztucznej inteligencji (33 vs 21%), mowy nienawiści, naruszenia ich godności osobistej, ośmieszenia, zastraszenia (23 vs 16%).

Najmniej bezpiecznie czujemy się podczas korzystania z bankowości i płatności online (38%) czy robienia zakupów (36%). Trzech na 10 Polaków obawia się korzystania z poczty elektronicznej.

Około 1/4 Polaków jako mało bezpieczne aktywności uważa korzystanie z mediów społecznościowych (27%), komunikatorów (23%) czy e-administracji. Jedynie 14% ma obawy podczas korzystania ze stron dla dorosłych. Najmniej obawiamy się o swoje bezpieczeństwo podczas korzystania z rozrywki (filmy i seriale, muzyka, książki) czy rozwijania swoich pasji (3%).Jedynie 7% obawia się zezwolenia dzieciom czy rodzinie na korzystanie ze służbowego sprzętu. Również aktywność na serwisach bukmacherskich nie wzbudza u nas zbyt dużych obaw (10%). Największe różnice można zaobserwować z punktu widzenia wykształcenia. Polacy z wyższym wykształceniem znacząco częściej niż posiadający wykształcenie podstawowe obawiają się o swoją aktywność w internecie podczas robienia zakupów (46 vs 21%), korzystania z bankowości online (43 vs 28%) czy mediów społecznościowych (33 vs 23%).

Niski poziom wiedzy o cyberbezpieczeństwie skutkuje tym, że ponad połowa Polaków nie wie, komu ufać w sieci, ani czy ich urządzenia, konta i aplikacje są tak naprawdę bezpieczne. Czterech na 10 Polaków nie nadąża za zmianami w cyfryzacji stąd popełnia błędy i jest podatna na działania oszustów. Trzech na 10 Polaków jest zagubionych, bo kwestie cyberbezpieczeństwa są zbyt skomplikowane. Blisko 1 na 3 Polaków stwierdza, że zasady cyberbezpieczeństwa utrudniają im pracę lub aktywność w sieci. Kobiety zdecydowanie częściej niż mężczyźni odpowiedziały twierdząco na wszystkie przedstawione opinie w badaniu, podobnie osoby starsze. Nie zaobserwowano większych różnic wśród respondentów z uwagi na miejsce zamieszkania.

2.3.

Jak jesteśmy atakowani i oszukiwani w internecie?

Jedynie 14% Polaków czuje się niezagrożonych cyberatakami. Aż 4 na 10 Polaków ocenia zmaterializowanie się takiego ryzyka za wysoce prawdopodobne. Co więcej, 36% Polaków osobiście doświadczyło cyberataków lub oszustw w internecie lub incydentów cyberbezpieczeństwa w przeciągu ostatniego roku. Częściej byli to mężczyźni (41 vs 31%), osoby mieszkające na wsi (40 vs 28%). Najczęstszą formą ataku był phishing (41%), scam (38%) oraz spoofing (27%). W co piątym przypadku było to przejecie konta (np. w mediach społecznościowych, e-sklepie, forum itp.). Osoby z wyższym wykształceniem częściej niż osoby z podstawowym wykształceniem wskazały, że doświadczyły phishingu (55 vs 26%), spoofingu (31 vs 12%) czy wyciekły ich dane osobowe (12 vs 3%). Osoby z wykształceniem podstawowym częściej wskazały, że doświadczyły scamu (49 vs 31%), kradzieży tożsamości (18 vs 2%) czy złośliwego oprogramowania (23 vs 9%).

Prawie 1/3 Polaków kiedykolwiek otrzymała informację o kradzieży lub wycieku danych osobowych. Częściej byli to mężczyźni, młodsze osoby (18–39 lat) oraz z wyższym wykształceniem.

Po podaniu definicji scamu ponad połowa (56%) Polaków przyznała, że osobiście doświadczyła scamu. Częściej byli to mężczyźni (59 vs 53%), osoby młodsze (68 vs 43%) czy z wyższym wykształceniem (66 vs 45%). Najczęściej natrafiono na scam poprzez fałszywy e-mail (50%) lub SMS czy MMS (37%), fałszywa wiadomość na komunikatorze internetowym (29%). Co czwarty scam to fałszywa reklama czy zakup. Jedynie 17% doświadczyło scamu rzadziej niż kilka razy w roku. Do najczęstszych rodzajów scamów, jakich doświadczono, można zaliczyć fałszywy konkurs lub loterię (41%), oszustwo phishingowe (39%), oszustwo zakupowe (34%) czy możliwość dodatkowego zarobkowania (26%) i inwestowania (20%). Z kolei 16% scamów to fałszywa akcja dobroczynna. Ponad 1/4 z tych osób natrafia na scam przynajmniej raz w tygodniu lub częściej.

Polacy pesymistycznie postrzegają kwestię skali scamu – jedynie 6% Polaków nie zaobserwowało wzrostu scamu w ostatnich latach. Czterech na 10 uważa, że skala scamu rośnie nieprzerwanie, a 8%, że wzrosła najbardziej od czasu wojny w Ukrainie lub ChatGPT. Na pandemię jako źródło wzrostu wskazało 18%. Wzrost scamu zaobserwowały szczególnie osoby z wyższym wykształceniem (46 vs 32%) oraz mężczyźni (47 vs 36%). Co gorsza, 8 na 10 Polaków uważa, że zjawisko scamu nasili się w kolejnych pięciu latach. Ponownie częściej z tą opinią zgadzają się mężczyźni i osoby z wyższym wykształceniem.

Aż 73% Polaków popiera pomysł uregulowania kar nakładanych na duże platformy internetowe w związku z brakiem lub powolnym czasem reakcji na oszustwa internetowe takie jak np. fałszywe reklamy. Częściej chcą tego osoby z dużych miast (85 vs 71%) oraz z wyższym wykształceniem (82 vs 64%).

Nieostrożność ludzi (59%), nieodpowiednie zabezpieczenie systemów i urządzeń (48%) oraz brak wiedzy lub szkoleń (46%) są najczęstszymi czynnikami sprzyjającymi cyberprzestępczości z perspektywy konsumenta/obywatela. Jedynie co piąty wskazał na brak pieniędzy. Około 25% twierdzi, że czynnikiem sprzyjającym cyberprzestępczości jest brak czas na zadbanie o cyberbezpieczeństwo czy wymóg posiadania zbyt wielu kont w internecie, w których wiele osób się gubi.

2.4.

Jakie mamy złe nawyki z zakresu cyberbezpieczeństwa?

Spora część polskiego społeczeństwa mało ostrożnie podchodzi do kwestii bezpiecznego korzystania z internetu. Co piąty Polak deklaruje trzynaście z trzydziestu trzech badanych złych nawyków. Nadal co czwarty Polak używa tego samego hasła w wielu miejscach i serwisach. Do najpopularniejszych nawyków można zaliczyć stosowanie profilowanej reklamy (37%), brak zdobywania wiedzy o cyberzagrożeniach (29%), niekorzystanie z przeglądarki w trybie prywatnym (28%) czy brak śledzenia aktualnych trendów o dezinformacji czy cyberprzestępczości (26%). Mniej niż 10% Polaków deklaruje otwieranie załączników z e-maili pochodzących z niezaufanych źródeł, brak kasowania swoich danych z elektroniki w momencie sprzedaży czy wynajmu, klikania w linki bez patrzenia na szczegółowy adres nadawcy czy wykorzystania sprzętu służbowego do celów prywatnych.

Na bazie naszego testu i innych odpowiedzi można śmiało wskazać, że popularność złych nawyków w rzeczywistości jest zaniżona i głównie deklaratywna.

Bardzo mało, bo zaledwie 10% społeczeństwa brało udział w kampanii zwiększającej świadomość i wiedzę na temat cyberbezpieczeństwa. 42% spośród tych osób samodzielnie się dokształcało, 27% natomiast z nich uczestniczyło w szkoleniu zorganizowanym przez pracodawcę. Kampanie rządowe czy też kampanie organizowane przez firmy (np. bank) były źródłem edukacji dla 13% wszystkich uczestników takich kampanii. Mężczyźni częściej niż kobiety deklarowali, że sami się dokształcają (49 vs 32%).Kobiety częściej niż mężczyźni brały udział w kampaniach rządowych, spotach emitowanych w mediach.

2.5.

Jak dbamy o bezpieczeństwo i przetwarzanie naszych danych?

Co drugi Polak przechowuje dane na urządzeniach elektronicznych takich jak stacjonarny komputer, laptop (49%) czy smartfon, tablet (47%). Co trzeci na pamięciach przenośnych, a co czwarty w chmurze. Jedynie 7% Polaków korzysta z dysków sieciowych (typu NAS). Kobiety częściej drukują kluczowe dokumenty (16 vs 7%), a młodzi częściej niż starsi trzymają dane w chmurze (33 vs 16%).

Sześciu na 10 Polaków nie wykonuje lub nie wie, czy wykonuje zapasową kopię swoich kluczowych danych. Kopię bezpieczeństwa (tzw. backup) częściej wykonują mężczyźni (44 vs 37%), osoby młode (46 vs 33%) z wyższym wykształceniem (50 vs 41%).

Wśród Polaków powszechnie (90%) znane jest Rozporządzenie o Ochronie Danych Osobowych (RODO). Zdania są natomiast podzielone w kwestii tego, czy wprowadzenie RODO zwiększyło ich poczucie bezpieczeństwa w zakresie prywatności danych osobowych i ich przetwarzania. Podczas gdy 38% Polaków zgadza się z tą tezą, niemalże taki sam odsetek (37%) nie odczuł zwiększenia poczucia bezpieczeństwa, a jedna czwarta naszego społeczeństwa nie ma zdania na ten temat.

Polacy źle oceniają nasze społeczeństwo w zakresie ochrony swoich danych osobowych. Siedmiu na 10 badanych ocenia, że Polacy zbyt nieostrożnie zostawiają swoje dane osobowe w internecie. Tego zdania są częściej osoby starsze (80 vs 70%).

2.6.

Czy doświadczamy mowy nienawiści i jak ją ograniczyć?

Co trzeci Polak osobiście doświadczył mowy nienawiści. Częściej spotkało to mężczyzn (42 vs 28%), osoby młode (50 vs 23%) czy z podstawowym wykształceniem (40 vs 31%).

Ponad 7 na 10 Polaków uważa, że w sieci jest zbyt dużo mowy nienawiści. Podobnie 7 na 10 Polaków uważa, że należy dokonać zmian w kodeksie karnym i uregulować prawnie walkę z mową nienawiści, gdyż dziś np. nie ma w nim definicji hejtu. Obie opinie częściej deklarują kobiety (ok. 80 vs 67%), osoby młodsze czy z wyższym wykształceniem (83 vs 67%).

Blisko 2 na 3 Polaków popiera wprowadzenie do porządku prawnego tzw. ślepego pozwu w celu walki z anonimowym hejtem w sieci. Częściej poparcie deklarują kobiety (67 vs 61%) i osoby z wyższym wykształceniem (76 vs 52%).

2.7.

Jak zadbać o ochronę dzieci i młodzieży w internecie?

56% Polaków uważa, że polskie prawo nie chroni odpowiednio dzieci przed treściami dla dorosłych w internecie ze względu na nierzetelne sprawdzanie pełnoletności. Dziś bowiem można wejść do serwisu z treściami pornograficznymi w internecie i samemu deklarować, że ma się 18 lat. Z tą opinią częściej zgadzały się osoby będące bardziej aktywne w internecie, w większych gospodarstwach domowych (67 vs 49%), gdzie 67% dotyczy gospodarstw, w których są minimum 4 osoby, a 49% dotyczy jednoosobowych gospodarstw domowych), posiadające dzieci (63 vs 53%). Były to też częściej kobiety (60 vs 52%), osoby młodsze (66 vs 44%) i z podstawowym wykształceniem (57 vs 43%).

Trzech na 4 Polaków twierdzi, że zakazy ze świata rzeczywistego (np. zakaz sprzedaży alkoholu/energetyków/treści pornograficznych dzieciom w sklepie) powinny obowiązywać i być egzekwowane także w internecie (np. zakaz dostępu dla dzieci do treści pornograficznych przez internet). Częściej deklarowały to kobiety i osoby z wyższym wykształceniem.

Jedynie 3 na 10 Polaków poprawnie odpowiedziało na pytanie dotyczące minimalnego wieku uprawniającego do założenia konta w mediach społecznościowych. Co piąty nie wiedział, że w ogóle istnieje taki limit.

Widoczne jest duże poparcie (73%) dla wprowadzenia rzetelnej weryfikacji wieku zamiast dobrowolnych deklaracji. Gdyby takie rozwiązanie miało zostać wprowadzone, najważniejszą kwestią byłby bezpieczny mechanizm odporny na wszelkie wycieki danych (48%). Dla 39% zwolenników rzetelnej weryfikacji wieku ważne byłoby stworzenie i wykorzystanie cyfrowego certyfikatu wieku (np. 18+) bez danych osobowych. Taki sam odsetek badanych twierdzi, że powinno się wprowadzić prawo wymuszające na platformach internetowych skorzystanie z rozwiązań oferujących anonimową weryfikację wieku pod groźbą zakazania prowadzenia działalności w Polsce.

Respondenci pytani o jeszcze inne dodatkowe metody zwiększenia bezpieczeństwa dzieci najczęściej wskazywali na potrzebę ustalenia przez rodziców wspólnie z dzieckiem zasad bezpiecznego korzystania z internetu (35%), wprowadzenie do szkół obowiązkowych lekcji z zakresu bezpieczeństwa online (34%) oraz ograniczenie czasu spędzanego przed ekranem przez dzieci i młodzież, zarówno w domu, jak i w środowisku szkolnym (33%). 27% popiera zakazanie korzystania z elektroniki w przedszkolach i wybranych klasach szkoły podstawowej.

Co drugi rodzic posiadający dziecko poniżej 18. roku życia deklaruje stosowanie kontroli rodzicielskiej na urządzeniach elektronicznych. Czterech na 5 rodziców wykorzystujących kontrolę rodzicielską stosuje ją na smartfonie, a następnie komputerze (34%).

2.8.

Czy ważny jest dla nas kraj pochodzenia dostawcy rozwiązań z zakresu cyberbezpieczeństwa?

Połowa Polaków deklaruje, że przy kupnie lub korzystaniu z rozwiązań z zakresu cyberbezpieczeństwa ważny jest kraj pochodzenia dostawcy (np. antywirusa). Aż co trzeci jednak nie ma zdania w tej kwestii, a dla 20% nie jest to istotne. Takie podejście kontrastuje trochę z polityką zakupową konsumentów, którzy ochoczo kupują rozwiązania od dostawców spoza Polski, a szczególnie Azji. Siedmiu na 10 badanych, dla których kwestia kraju pochodzenia jest ważna, preferuje dostawców z Polski. Dużym zaufaniem cieszą się również kraje anglosaskie (43%) oraz inne należące do Unii Europejskiej (39%). Co ciekawe, Izrael czy Korea Południowa cieszą się podobnym zaufaniem jak Chiny, Indie czy Rosja, sięgające pojedynczych punktów procentowych.

2.9.

Jak cyberbezpieczny jest nasz kraj?

Ocena priorytetowego traktowania w naszym państwie kwestii cyberbezpieczeństwa jest spolaryzowana: 33% Polaków uważa, że to zagadnienie nie jest priorytetem w Polsce, 29% twierdzi, że bezpieczeństwo w internecie jest traktowane priorytetowo. A ponad jedna trzecia (38%) nie ma zdania na ten temat.

Wśród dwóch z pięciu najpopularniejszych powodów incydentów w organizacjach w Polsce występuje czynnik ludzki – brak wiedzy wśród ludzi (28%) oraz niestosowanie się pracowników do polityk cyberbezpieczeństwa (24%). Równie ważnym powodem jest indywidualne działanie hakerów i profesjonalnych grup, w tym sponsorowanych przez obce służby. Na brak środków wskazało jedynie 16% badanych. Tylko 14% za główną przyczynę uznaje brak doraźnych i nieplanowanych kontroli ze strony firm, urzędów czy państwa.

Rosja i Stany Zjednoczone to dwa kraje, w których według Polaków ma dochodzić do największej skali cyberataków. Na Polskę wskazało 15% badanych, podobny odsetek co na Ukrainę czy Chiny. Jedynie ok. 5% badanych wskazało na Iran lub Izrael. Należy jednak zaznaczyć że zdaniem aż 46% respondentów na całym świecie występuje podobna skala ataków – niezależnie od kraju czy regionu.

Największe różnice w odpowiedziach można zaobserwować z punktu widzenia wieku respondenta. Osoby starsze zdecydowanie częściej wskazały niż osoby młodsze, że na całym świecie występuje podobna skala cyberataków (59 vs 34%). Podobnie częściej wskazano na Unię Europejską jako częstszy cel ataków (15 vs 9%). Osoby młodsze częściej wskazały, że skala ataków jest większa w Ukrainie (22 vs 10%), Iranie (12 vs 3%), USA (25 vs 17%) czy w Polsce (17 vs 9%).

1. SPOŁECZEŃSTWO 5.0, CZYLI ZRÓWNOWAŻONEGO ROZWOJU DZIĘKI TECHNOLOGII

Współczesne społeczeństwa stoją przed wyzwaniem – czy osiągnęły szczyt swojego rozwoju?

Ostatnie dekady przyniosły szereg problemów: zakłócenia w łańcuchach dostaw, rosnącą inflację, zmiany klimatu i spowolnienie wzrostu gospodarczego. W odpowiedzi na te wyzwania, w latach 80. XX wieku, narodziła się idea zrównoważonego rozwoju. Jej celem jest znalezienie równowagi między postępem ekonomicznym, ochroną środowiska i rozwojem społecznym. Koncepcja ta kładzie nacisk na odpowiedzialne zarządzanie globalnymi dobrami publicznymi, takimi jak wiedza, środowisko naturalne, dziedzictwo kulturowe czy prawo do pokoju i zaspokajania podstawowych potrzeb. Inspiracją dla tej idei były prognozy zawarte w raporcie Klubu Rzymskiego „Granice wzrostu". Kluczem do realizacji tej wizji jest 17 Celów Zrównoważonego Rozwoju (SDG), ujętych w Agendzie 2030. Ten ambitny plan, przyjęty przez wszystkie państwa członkowskie ONZ w 2015 roku, wyznacza 169 konkretnych zadań mających na celu harmonijny rozwój w sferze gospodarczej, społecznej i środowiskowej.

Jak przyspieszyć wdrażanie tych celów i wspomóc rozwój społeczeństwa?

Eksperci wskazują na kluczową rolę rozwoju i wykorzystania usług cyfrowych i technologii. Badania japońskiej firmy Fujitsu pokazują, że liderzy w tej dziedzinie odkrywają potencjał łączenia cyfryzacji, nowoczesnych technologii i procesów z ludzkimi potrzebami, aby urzeczywistnić ideę zrównoważonego rozwoju. Kluczowe znaczenie ma wykorzystanie nowych technologii, takich jak sztuczna inteligencja, internet rzeczy czy analiza big data, w połączeniu z nowoczesną infrastrukturą telekomunikacyjną. Te innowacje mogą przyczynić się do rozwoju odnawialnych źródeł energii, redukcji emisji gazów cieplarnianych, tworzenia zrównoważonych miast i poprawy jakości edukacji. Przykłady zastosowań nowych technologii są liczne: autonomiczny transport może rozwiązać problem braku kierowców i wykluczenia transportowego, zaawansowane czujniki internetu rzeczy umożliwiają monitorowanie jakości wód, a technologia cyfrowych bliźniaków pomaga w optymalizacji funkcjonowania miast. Sztuczna inteligencja może usprawnić służbę zdrowia, skracając kolejki do lekarzy i automatyzując procesy administracyjne. Jednak sama technologia nie wystarczy - kluczowa jest zmiana podejścia społeczeństwa. Potrzebna jest nie tylko świadomość ekologiczna, ale przede wszystkim gotowość do korzystania z nowych technologii i cyfryzacji. Bez tego trudno będzie zrealizować ambitną wizję zrównoważonego rozwoju.

Japonia wyznacza kierunek – społeczeństwo 5.0

Japonia jawi się jako pionier w kształtowaniu cyfrowej przyszłości proponując model społeczeństwa 5.0 jako drogę do zrównoważonego rozwoju. Koncepcja ta zakłada stworzenie nowoczesnego społeczeństwa, w którym człowiek znajduje się w centrum, a jego jakość życia jest zdecydowanie wyższa dzięki wykorzystaniu nowoczesnych technologii. Kluczowym aspektem tej wizji jest harmonijne połączenie świata cyfrowego z rzeczywistością. Realizacja tego celu ma opierać się na wykorzystaniu najnowocześniejszych rozwiązań, takich jak sztuczna inteligencja, analiza big data, internet rzeczy, hiperłączność oraz robotyka i automatyzacja. Symbioza tych dwóch sfer ma umożliwić zrównoważony rozwój gospodarczy i efektywne rozwiązywanie globalnych wyzwań poprzez innowacyjne podejście społeczno-technologiczne. Plan japoński, przyjęty w 2016 roku, zakłada ewolucję od przemysłu 4.0 do społeczeństwa 5.0, gdzie zaawansowane technologie kształtują wszystkie aspekty życia społecznego, w tym sektor przemysłowy. Ta strategia jest odpowiedzią na specyficzne wyzwania Japonii, takie jak niedobory energetyczne, ograniczone zasoby naturalne i starzejące się społeczeństwo. Japoński model podkreśla kluczową rolę sztucznej inteligencji i robotyki w rozwiązywaniu długoterminowych problemów. Eksperci zwracają uwagę, że wobec rosnącej ilości danych, AI staje się niezbędna do podejmowania szybkich i trafnych decyzji.

Co charakteryzuje społeczeństwo 5.0?

To społeczeństwo ceniące innowacyjność i otwartość, pozbawione barier międzypokoleniowych, wykorzystujące nowe technologie do rozwiązania palących problemów ludzkości. Japończycy podkreślają, że kluczem do osiągnięcia tego modelu jest współpraca między biznesem, państwem i sektorem pozarządowym, zarówno na poziomie krajowym, jak i globalnym.

Zachęcenie społeczeństwa do korzystania z technologii

W Polsce, Fundacja Digital Poland jako pierwsza podjęła się regularnego badania gotowości Polaków do przyjęcia koncepcji społeczeństwa 5.0. Fundacja dostrzega w tym modelu potencjalne rozwiązanie dla wielu wyzwań stojących przed Polską, które są podobne do tych w Japonii - starzejące się społeczeństwo, niska dzietność czy problemy w sektorze energetycznym, coraz trudniejszy dostęp do lekarza i drożejąca ochrona zdrowia.

Choć nowoczesne technologie są dziś łatwo dostępne, wyzwaniem pozostaje zachęcenie Polaków do ich aktywnego wykorzystywania. Cóż nam z sieci 5G czy sztucznej inteligencji jeśli ludzie będą się ich obawiać? To właśnie społeczeństwo i jego gotowość do skorzystania z nowych rozwiązań stanowi centralny punkt badań Fundacji Digital Poland prowadzonych nieprzerwanie już od sześciu lat.

Trzy filary społeczeństwa 5.0

Koncepcja Społeczeństwa 5.0 opiera się na trzech filarach innowacji społecznych: danych, informacjach i wiedzy, z kluczową rolą sztucznej inteligencji (AI) w ich przetwarzaniu.

Dane – fundamenty cyfrowego świata

Dane to surowe fakty z rzeczywistości, zarówno materialnej, jak i niematerialnej, przedstawione w formie liczbowej, stanów, nazw czy kodów binarnych. Przykładowo w hipotetycznym mieście A, dane mogłyby obejmować szczegóły z rejestru mieszkańców, takie jak płeć, struktura gospodarstw domowych czy adresy. To właśnie te podstawowe elementy są gromadzone w cyberprzestrzeni.

Informacje – dane nabierają znaczenia

Kiedy dane zostają wyselekcjonowane i przetworzone w konkretnym celu, stają się informacjami. Wracając do przykładu miasta A, analiza danych demograficznych w czasie może ujawnić trendy populacyjne, tworząc wartościowe informacje o rozwoju miasta. To właśnie kontekst i cel analizy transformuje surowe dane w użyteczne informacje.

Wiedza – klucz do podejmowania decyzji

Wiedza powstaje, gdy informacje są dogłębnie zrozumiane, przeanalizowane i powiązane z ogólnymi zasadami czy najlepszymi praktykami. W przypadku miasta A, wiedza pozwoliłaby zrozumieć przyczyny zmian demograficznych i zaproponować skuteczne rozwiązania. Wiedza umożliwia wyciąganie wniosków i podejmowanie świadomych decyzji bazujących na dostępnych informacjach.

Społeczeństwo oparte na wiedzy – nowa era przetwarzania danych

Dotychczas proces przekształcania danych w wiedzę wymagał interakcji człowieka z komputerem. Jednakże w społeczeństwie 5.0 ta transformacja będzie zachodzić automatycznie, bez bezpośredniej ingerencji ludzkiej. Rola człowieka ograniczy się do korzystania z wiedzy wygenerowanej przez AI, będącej efektem końcowym procesu przetwarzania danych. Ta ewolucja w kierunku społeczeństwa opartego na wiedzy oznacza fundamentalną zmianę w sposobie, w jaki przetwarzamy i wykorzystujemy informacje. AI staje się kluczowym elementem w procesie przekształcania surowych danych w użyteczną wiedzę, otwierając nowe możliwości dla innowacji i rozwiązywania problemów społecznych.

Rewolucja społeczna w erze wiedzy – co nas czeka?

Japonia, podobnie jak inne kraje rozwinięte, przeszła ewolucję od społeczeństwa opartego na pracy fizycznej do modelu skupionego na kapitale i zaawansowanych technologiach. Ta transformacja, napędzana rewolucją przemysłową, doprowadziła do koncentracji produkcji i konsumpcji w ośrodkach miejskich, często zlokalizowanych wokół portów i lotnisk. Jednak koncepcja społeczeństwa 5.0 proponuje kolejny przełom – przejście do modelu, w którym głównym źródłem wartości staje się wiedza. W tym nowym paradygmacie, kluczowe znaczenie zyskują nie tyle skupiska dóbr materialnych, co przestrzenie wiedzy – miejsca, gdzie dane i informacje są gromadzone, analizowane i przekształcane w użyteczną wiedzę. W tym procesie nieocenioną rolę odgrywa sztuczna inteligencja, stając się katalizatorem społeczeństwa opartego na wiedzy. Ta nowa era otwiera fascynujące możliwości. Integracja danych i informacji może prowadzić do powstania innowacji zdolnej zrewolucjonizować nie tylko sektor usług, ale także tradycyjne gałęzie gospodarki, takie jak rolnictwo czy przemysł wytwórczy. Przykładowo, japońskie rolnictwo, dotychczas borykające się z nieefektywnością wynikającą z rozproszenia gruntów, może doświadczyć odrodzenia dzięki wykorzystaniu zaawansowanych technologii – od precyzyjnych danych przestrzennych i prognoz pogody, po drony i roboty rolnicze.

Społeczeństwo oparte na wiedzy ma potencjał nie tylko do optymalizacji istniejących sektorów, ale także do kreowania zupełnie nowych gałęzi przemysłu, tym samym przekształcając strukturę całej gospodarki. Ta zmiana paradygmatu stawia nowe wyzwania przed organizacjami, które dotychczas odgrywały kluczową rolę w rozwoju technologicznym. O ile wcześniej ich głównym zadaniem było zwiększanie wartości dóbr materialnych, o tyle w społeczeństwie opartym na wiedzy będą musiały skupić się na wspieraniu rozwoju nowych sektorów gospodarki, generujących wartość dodaną w oparciu o wiedzę i innowacje.

1.1.

Strategiczne wyzwania stojące przed Polską

Najważniejsze wyzwania stojące przed Polską

Nadal najbardziej palącymi problemami w oczach Polaków są kwestie związane ze złym stanem systemu ochrony zdrowia, panującą drożyzną, starzejącym się społeczeństwem, panującą w urzędach biurokracją i ograniczonym dostępem osób młodych do mieszkań. Ważną kwestią stała się również ochrona środowiska.

81%	Zbyt długie kolejki do lekarza i szpitala
80%	Utrzymująca się drożyzna
78%	Starzenie się społeczeństwa
77%	Duża biurokracja w urzędach
75%	Ograniczony dostęp do mieszkań dla młodych Polaków

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Problemy z innowacyjnością czy cyfryzacją nie spędzają snu z powiek Polaków

W pierwszej dwudziestce wyzwań znalazły się jedynie dwa wyzwania związane wprost z cyfryzacją – brak inwestowania w kwalifikacje pracowników (69%) i brak edukacji medialnej przez co społeczeństwo jest podatne na dezinformację (67%).

Wyzwania związane z innowacyjnością znalazły się w trzeciej i czwartej dziesiątce rankingu, a kwestia uzależnienia od bigtech na 33. miejscu.

W ocenie Polaków nie jesteśmy celem zbyt wielu cyberataków w internecie (42. miejsce).

Większość wyzwań związanych z cyfryzacją znajduję się dopiero w czwartej i piątej dziesiątce rankingu.

Na ostatnich pozycjach znalazły się wyzwania związane z realizacją Cyfrowej Dekady 2030 takich jak brak umiejętności cyfrowych (50%), brak dostępu do szybkiego internetu (49%), zbyt mało specjalistów ICT (38%), brak możliwości załatwiania spraw przez internet (49%).

Największe wzrosty i spadki w rankingu strategicznych wyzwań

Największe spadki

- Obawy o podporządkowanie mediów celom politycznym (o dziewiętnaście pozycji, na 25. miejsce)
- Braku rządów prawa w Polsce (o dziewiętnaście pozycji, na 48. miejsce)
- Obawy o bankructwo systemu emerytalnego (o trzynaście pozycji, na 27. miejsce)
- Obawy o brak ochrony podstawowych wolności jednostki (o dwanaście pozycji, na 45. miejsce)

Największe wzrosty

- Zaniepokojenie nierównościami społeczno-finansowymi (o jedenaście pozycji, na 11. miejsce)
- Niewystarczające inwestycje pracodawców w kwalifikacje pracowników (o jedenaście pozycji, na 16. miejsce)
- Wzrost zanieczyszczenia środowiska naturalnego (o sześć pozycji, na 10. miejsce)
- Ograniczony dostęp młodych osób do mieszkań (o pięć pozycji, na 5. miejsce)

Ranking największych wyzwań stojących przez Polską (1-21)

	Procent Polaków zgadzających się ze zdaniem	RANKING	Różnica w rankingu vs 2023
TOP 11 PROBLEMÓW			
Coraz dłużej czeka się w Polsce na wizytę u lekarza lub zabieg w szpitalu	81	1	+4
W Polsce panuje drożyzna, zbyt rosną ceny produktów i usług	80	2	-1
Polskie społeczeństwo się starzeje, jest coraz więcej osób mających 60 lub więcej lat	78	3	-1
W urzędach jest za duża biurokracja	77	4	0
Młodzi Polacy mają ograniczony dostęp do mieszkań	75	5	+5
Podziały polityczne między Polakami są zbyt duże	74	6	-3
Polski system opieki zdrowotnej działa bardzo słabo, brakuje nowoczesnych leków i terapii	74	7	0
Podatki nie przekładają się na jakość usług publicznych	74	8	+3
W Polsce zbyt wiele ścieków trafia do rzek i jezior	72	9	+3
Rośnie zanieczyszczenie środowiska naturalnego w Polsce	71	10	+6
W Polsce jest zbyt wysoki poziom nierówności społeczno-finansowych	71	11	+11
TOP 12-21 PROBLEMÓW			
W Polsce zbyt wiele dorosłych i dzieci ma nadwagę	70	12	-4
W Polsce rodzi się zbyt mało dzieci	70	13	-4
Brakuje obiektywnych i niezależnych od władzy urzędników	70	14	+1
Polskie przedsiębiorstwa za mało korzystają z surowców wtórnych, w tym produktów z recyclingu	69	15	+5
Pracodawcy nie inwestują wystarczająco w rozwój i kwalifikacje swoich pracowników	69	16	+11
W Polsce zbyt wiele osób jest samotnych i nastąpił rozpad więzi społecznych	68	17	0
Brakuje w Polsce edukacji medialnej przez co społeczeństwo podatne jest na dezinformację	67	18	-5
Pogoda w Polsce jest coraz bardziej uciążliwa – coraz częściej mamy do czynienia z suszami, powodziami, wysokimi temperaturami	67	19	-1
W Polsce zbyt mało produkuje się energii z odnawialnych źródeł, takich jak fotowoltaika, wiatraki	65	20	-1
W Polsce brakuje przemyślanej i odpowiedzialnej polityki imigracyjnej	65	21	+2

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Ranking największych wyzwań stojących przez Polską (22-50)

TOP 22-50 PROBLEMÓW

	Procent Polaków zgadzających się ze zdaniem	RANKING	Różnica w rankingu vs 2023
Polska za bardzo opiera swoją energetykę na węglu, przez co prąd będzie drożał	64	22	2 ↑
W Polsce jest za mało stacji ładowania pojazdów elektrycznych i stacji ładowania aut na wodór	64	23	/brak w 2023/
W Polsce za mało wspiera się rozwój technologiczny, badania i innowacyjność	63	24	-3 ↓
Media w Polsce są podporządkowane celom politycznym	62	25	-19 ↓
Polacy są zbyt mało otwarci na osoby o innym kolorze skóry, wyznaniu religijnym, orientacji	62	26	2 ↑
System emerytalny może w przyszłości zbankrutować	61	27	-13 ↓
W Polsce panuje zbyt duży poziom korupcji i łapówkarstwa	61	28	2 ↑
Bezpieczeństwo Polski nie jest wspierane nowoczesnymi technologiami w wystarczającym stopniu	61	29	3 ↑
Polacy zbyt mało uczą się przez całe życie i nie są gotowi do przekwalifikowania się	61	30	5 ↑
W Polsce brakuje dostępu do rzetelnych informacji	60	31	-5 ↓
Polacy jedzą zbyt dużo mięsa i odżywiają się niezdrowo	59	32	-7 ↓
Polska gospodarka może zostać zdominowana i uzależniona od cyfrowych gigantów takich jak Apple, Amazon, Google, Facebook	58	33	/brak w 2023/
Polacy nie mają dostępu do całej swojej dokumentacji medycznej w formie cyfrowej przez internet	57	34	-3 ↓
W Polsce brakuje dostępu do dobrej infrastruktury transportowej, wodociągowej, energetycznej	57	35	5 ↑
Przemysł w Polsce wykorzystuje przestarzałe, brudne i mało przyjazne środowisku technologie	56	36	0 =
W Polsce nie wszędzie można zapłacić bezgotówkowo (cyfrowo)	53	37	2 ↑
Firmy w Polsce nie wykorzystują wystarczająco cyfryzacji i nowych technologii	53	38	3 ↑
Poziom edukacji w polskich szkołach (podstawowych, zawodowych, licealnych) jest na niskim poziomie	53	39	4 ↑
W Polsce zbyt mało wykorzystuje się cyfryzację i zaawansowane technologie	52	40	-6 ↓
Polska jest nieznaczącym producentem elektroniki, w tym półprzewodników	52	41	-3 ↓
Polska i polskie społeczeństwo jest przedmiotem zbyt wielu cyberataków w internecie	52	42	/brak w 2023/
W Polsce nie działa dobrze transport publiczny – autobusy, pociągi, komunikacja miejska	50	43	-1 ↓
Polskie społeczeństwo nie posiada wystarczających umiejętności cyfrowych, w tym komputerowych	50	44	2 ↑
W Polsce nie są chronione podstawowe wolności jednostki	49	45	-12 ↓
Spraw urzędowych nie można załatwić w wygodny sposób przez internet	49	46	-2 ↓
Zbyt mało Polaków ma dostęp do superszybkiego Internetu	49	47	-2 ↓
W Polsce nie ma rządów prawa	47	48	-19 ↓
W Polsce brakuje rąk do pracy, jest za mało pracowników	45	49	-2 ↓
W Polsce jest zbyt mało informatyków	38	50	-1 ↓

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Nie odnotowano diametralnych różnic pomiędzy kobietami, a mężczyznami patrząc na wskazania na najważniejszych dziesięć wyzwań przed jakimi stoi nasz kraj.

Warto jednak zauważyć, że kobiety częściej niż mężczyźni wskazywały na następujące wyzwania: rosnące zanieczyszczenie środowiska naturalnego (74 vs 68%), zbyt duży poziom korupcji i łapówkarstwa (65 vs 56%), niezdrowe odżywianie i spożywanie zbyt dużej ilości mięsa (63 vs 55%), brak wszechobecnej możliwości bezgotówkowych płatności (56 vs 49%) oraz brak przemyślanej polityki imigracyjnej (68 vs 62%).

Natomiast mężczyźni znacząco częściej wskazywali na problemy dotyczące zbyt małej produkcji elektroniki (60 vs 44%), zbyt małego wykorzystania cyfryzacji i technologii (59 vs 44%), zbyt małej liczby stacji ładowania pojazdów elektrycznych, aut na wodór (71 vs 57%), braku edukacji medialnej i podatności na dezinformację (74 vs 61%), małej liczby pracowników (52 vs 39%) oraz podporządkowania mediów celom politycznym (68 vs 57%).

WIEK

Starsze osoby, w wieku ponad 60 lat, znacząco częściej niż najmłodsi Polacy, w wieku 18-29, wskazywały na następujące strategiczne problemy: zbyt duże podziały polityczne między Polakami (87 vs 54%), brak przełożenia podatków na jakość usług publicznych (84 vs 56%), dużą biurokrację w urzędach (85 vs 58%), zbyt wysoki poziom nierówności społeczno-finansowych (78 vs 57%), starzejące się Polskie społeczeństwo (88 vs 68%) oraz brak przemyślanej polityki imigracyjnej (79 vs 45%), zbyt małą produkuję energii z odnawialnych źródeł (76 vs 49%), niski poziom korzystania przedsiębiorstw z surowców wtórnych (81 vs 56%), zbyt mały dostęp do superszybkiego internetu (58 vs 35%), zbyt małą liczbę rodzących się dzieci (80 vs 58%), niezdrowe odżywanie i jedzenie dużej ilości mięsa (66 vs 45%).

MIEJSCE ZAMIESZKANIA

Mieszkańcy największych miast (powyżej 500 tyś. mieszkańców) znacząco częściej niż mieszkańcy wsi dostrzegali takie wyzwania stojące przed Polską jak: słabo działający system opieki zdrowotnej (88 vs 69%), duże podziały polityczne między Polakami (86 vs 71%), podporządkowanie mediów celom politycznym (75 vs 61%), zbyt małą produkcję energii z odnawialnych źródeł (76 vs 64%), nadwagę dorosłych i dzieci (76 vs 65%), możliwe bankructwo systemu emerytalnego (68 vs 57%).

Z kolei mieszkańcy wsi częściej wskazywali na słabo działający transport publiczny (56 vs 45%), zbyt mały dostęp do superszybkiego Internetu (53 vs 44%), braki w Polskim społeczeństwie dotyczących umiejętności cyfrowych (53 vs 48%) oraz braki w dostępie do dobrej infrastruktury transportowej, wodociągowej, energetycznej (60 vs 55%).

WYKSZTAŁCENIE

Polacy z wyższym wykształceniem znacząco częściej niż posiadający podstawowe wykształcenie wskazywali na problem starzejącego się społeczeństwa (87 vs 54%), panującej drożyzny (79 vs 62%), zbyt małego wykorzystania surowców wtórnych, w tym produktów z recyklingu przez firmy z Polski (77 vs 58%), malejącą liczbę rodzących się dzieci (75 vs 46%), możliwość bankructwa systemu emerytalnego (67 vs 45%), brak przełożenia podatków na jakość usług publicznych (79 vs 53%), słabo działający system opieki zdrowotnej (77 vs 56%), podporządkowania mediów celom politycznym (66 vs 43%).

Jan Oleszczuk-Zygmuntowski

Współprzewodniczący, Polska Sieć Ekonomii

Polacy coraz częściej widzą, że gospodarka może produkuje coraz większe słupki PKB, ale nie zmienia się przez to jakość życia. Wyniki badania fundacji Digital Poland pokazują, że rośnie świadomość podstawowych problemów bytowych, takich jak szkodliwe nierówności, traktowanie pracowników przedmiotowo czy tragiczna sytuacja na rynku mieszkaniowym.

Jako Polska Sieć Ekonomii jesteśmy przekonani, że polski model rozwoju się wyczerpał. Dryf rozwojowy pozwala nam jeszcze unosić się na fali trendów makroekonomicznych, jak np. *friendshoring*, ale coraz większym kosztem społecznym. Korekta kursu staje się zaś coraz trudniejsza, gdy nie ma energii do poniesienia kosztów zmiany. Konsekwencje tego dryfu będą coraz bardziej widoczne w każdym roku, a za pięć lat staniemy przed koniecznością zmiany biegu z powodu końca obecnej perspektywy unijnej.

Bolączki, które według Polaków tracą na znaczeniu, mają przede wszystkim charakter polityczny i odnoszą się do praworządności czy narracji medialnej. Problemy ekonomiczno-społeczne z kolei zostają, trzeba mieć na nie bowiem konkretną ofertę, inną niż proste przestrzeganie prawa czy etyki. W istocie konieczne jest zaproponowanie nowego modelu rozwoju Polski, bardziej egalitarnego, opartego o kapitał społeczny i nowe technologie cyfrowe czy energetyczne.

Z danych wynika również, że to nie wiek i płeć jest najważniejszym podziałem w odniesieniu do problemów życiowych, ale klasa. Co ciekawe, podział miasto–wieś wydaje się słabszym wyznacznikiem niż poziom wykształcenia. Osoby z wykształceniem podstawowym wydają się mniej zaniepokojone usługami publicznymi, demografią czy inflacją niż lepiej wykształceni, być może bardziej obawiający się utraty tego, czego się już dorobili. Konieczne byłoby jednak głębsze spojrzenie w dane źródłowe, aby ocenić, co ma dla nich większe znaczenie niż dla grup lepiej wykształconych.

Warto też zauważyć, że niezmiennie na czele ważnych problemów Polski ląduje słabość systemu ochrony zdrowia. Jednocześnie jest to temat, który nie przekłada się na działania polityczne. Przywykliśmy jako społeczeństwo, że tego się „nie da" i radzimy sobie, płacąc ponad 50 mld zł z własnej kieszeni, zasypując w ten sposób lukę publicznego wydatkowania pogłębianą przez ponadpartyjne rozdawanie przywilejów podatkowych.

Słowo na koniec: bardzo cieszy, że traci na znaczeniu antypaństwowa propaganda, taka jak straszenie bankructwem ZUS. Polska jest, jak widać, gotowa na kolejny krok w rozwoju, czyli budowę zaufania i siły swoich instytucji. Wypracowanie nowego modelu rozwoju zaczyna się przecież od ulepszenia własnego mentalnego modelu świata.
I tu jestem optymistą.

dr Małgorzata Starczewska-Krzysztoszek

Wydział Nauk Ekonomicznych Uniwersytetu Warszawskiego, Towarzystwo Ekonomistów Polskich

Prowadzone od sześciu lat (2019–2024) badania „Technologie w służbie społeczeństwa. Czy Polscy zostaną społeczeństwem 5.0?" sugerują, że większość problemów wskazywanych jako najważniejsze jest nierozwiązywalna, bo sprawy mieszczące się w TOP10(11) są od lat niezmienne. System opieki zdrowotnej jest daleki od oczekiwań, wzrost cen ciągle uderza gospodarstwa domowe po kieszeniach, społeczeństwo się starzeje, administracja publiczna nie dostarcza nam dobrej jakości usług tylko biurokrację.

Problemu starzenia się społeczeństwa nie da się rozwiązać przy malejącej dzietności Polaków (współczynnik dzietności = 1,16 – 2023; 2,0 – 1990; GUS). Można jedynie stworzyć warunki do dłuższego życia w zdrowiu, które pozwoli na pozostawanie dłużej na rynku pracy, co przy malejącej populacji osób w wieku produkcyjnym ma i będzie miało coraz większe znaczenie dla gospodarki, ale też dla emerytów ze względu na malejącą stopę zastąpienia (relację emerytury do ostatniego wynagrodzenia). W 2022 r. oczekiwana długość życia w zdrowiu wynosiła dla 60-latków nieco ponad 10 lat dla mężczyzn i 11,5 roku dla kobiet (GUS). Jak jednak wydłużyć życie w zdrowiu, gdy system opieki zdrowotnej nie daje na to szans (w rankingu Badania problem wskazywany na miejscu 1. i 7.)? Wyniki badania dostarczają ciekawych odpowiedzi. Polacy pytani o otwartość na korzystanie z nowych technologii wskazują na udostępnianie instytucjom naukowym swoich anonimowych wyników badań medycznych w celu stworzenia nowych metod leczenia wybranych chorób (7. miejsce – 55% badanych), na noszenie specjalnych opasek monitorujących stan zdrowia i przesyłających informacje do lekarza (52% badanych), konsultacje u lekarza przez Internet (50%), możliwość wymiany organów na nowe, które zostały wydrukowane lub wyhodowane (46%), na operacje dokonywane przez roboty, a nie chirurga (33%), na diagnozy medyczne stawione przez sztuczną inteligencję, zamiast lekarza (31%). Czyli przeciętny Polak wie – odpowiedzią na dłuższe życie w zdrowiu jest cyfryzacja, są nowe technologie.

Rozwój i wykorzystanie cyfryzacji i nowych technologii to szansa na rozwiązanie większości problemów wskazywanych przez Polaków w badaniu. Aby lepiej panować nad inflacją, należy stosować coraz bardziej zaawansowane modele makroekonomiczne wymagające większej liczby danych, wydajniejszych komputerów i sztucznej inteligencji. Odbiurokratyzowanie urzędów i poprawa jakości świadczenia przez nie usług – też cyfryzacja i nowe technologie. Na załatwianie wszystkich spraw urzędowych i administracyjnych cyfrowo i zrezygnowanie z tradycyjnej, papierowej formy komunikacji otwartych jest 54% badanych. Ograniczanie zanieczyszczania środowiska – cyfryzacja i nowe technologie.

Jak jednak przyspieszyć procesy cyfryzacji i wdrażania nowych technologii, gdy „w Polsce za mało wspiera się rozwój technologiczny, badania i innowacyjność" (63% badanych wskazuje to jako problem), 61% mówi że Polacy niechętnie uczą się przez całe życie i nie są gotowi do przekwalifikowania się, 50% wskazuje na brak wystarczających umiejętności cyfrowych, w tym komputerowych Polaków.

Jak przyspieszyć procesy cyfryzacji i wdrażania nowych technologii, gdy także pracodawcy nie widzą potrzeby inwestowania w rozwój i kwalifikacje pracowników (ten problem wskazuje 69% badanych)? Mogłoby to istotnie przyspieszyć procesy zmian, tym bardziej że Polacy zaakceptowaliby (43%) analizę braków w umiejętnościach cyfrowych przez sztuczną inteligencję i stworzenie przez nią indywidualnych programów rozwoju.

Problemy mamy zidentyfikowane. Wiele ścieżek ich rozwiązywania – także. Teraz implementacja. Tak w drodze zmian regulacyjnych, wsparcia finansowego ze środków publicznych, zmian w procesie edukacji, zmian w podejściu firm do upskillingu, reskilingu… i zmian w naszej świadomości, w myśleniu, o znaczeniu cyfryzacji i nowych technologii dla naszej przyszłości. Z tym ostatnim niestety będzie najtrudniej.

Łukasz Kozłowski

Główny ekonomista, Federacja Przedsiębiorców Polskich

Wyniki tegorocznego badania po raz kolejny potwierdzają, że polskie społeczeństwo potrafi trzeźwo i przenikliwie ocenić główne wyzwania stojące przed naszym krajem, zarówno w perspektywie krótko-, jak i długoterminowej. Decydenci powinni ze szczególną uwagą zapoznać się z tymi informacjami, dostarczają one bowiem cennych wskazówek odnośnie do oczekiwanych przez społeczeństwo kierunków działań w sferze polityk publicznych.

W bieżącym roku wśród wskazywanych problemów na czoło wysuwa się coraz dłuższy okres oczekiwania w kolejce na konsultację lekarską lub zabieg. Dostępne dane potwierdzają, że faktycznie następuje niepokojące pogorszenie sytuacji w zakresie dostępności świadczeń opieki zdrowotnej. Jak wynika ze sprawozdania NFZ, między I kw. 2022 r. a I kw. 2024 r. liczba pacjentów oczekujących w kolejce do specjalisty zwiększyła się o 13%. Co gorsza, system przestaje sobie radzić z szybkim zapewnianiem świadczeń medycznych wtedy, gdy są one najbardziej potrzebne, gdyż w analogicznym okresie liczba czekających pacjentów w przypadkach pilnych wzrosła aż o 71%, a mediana czasu oczekiwania w przypadku wielu specjalności wzrosła ponad dwukrotnie!

Wszystko to dzieje się w kontekście głośno ogłaszanych zapowiedzi rychłego zwiększenia skali publicznego finansowania systemu ochrony zdrowia do poziomu 7% PKB, co pozwoliłoby nam na zrównanie się ze średnią unijną. Mając na uwadze rozdźwięk między tymi deklaracjami a rzeczywistością, zrozumiałe jest, że uczestnicy badania jeszcze częściej niż dotychczas jako poważny problem wskazują to, że podatki nie przedkładają się na jakość usług publicznych. Decydenci polityczni wykazują się dużą sprawnością we wprowadzaniu nowych instrumentów związanych z transferami społecznymi, budowa sprawnie funkcjonującego systemu oraz dostarczanie konkretnych usług publicznych pozostaje jednak nierozwiązanym problemem.

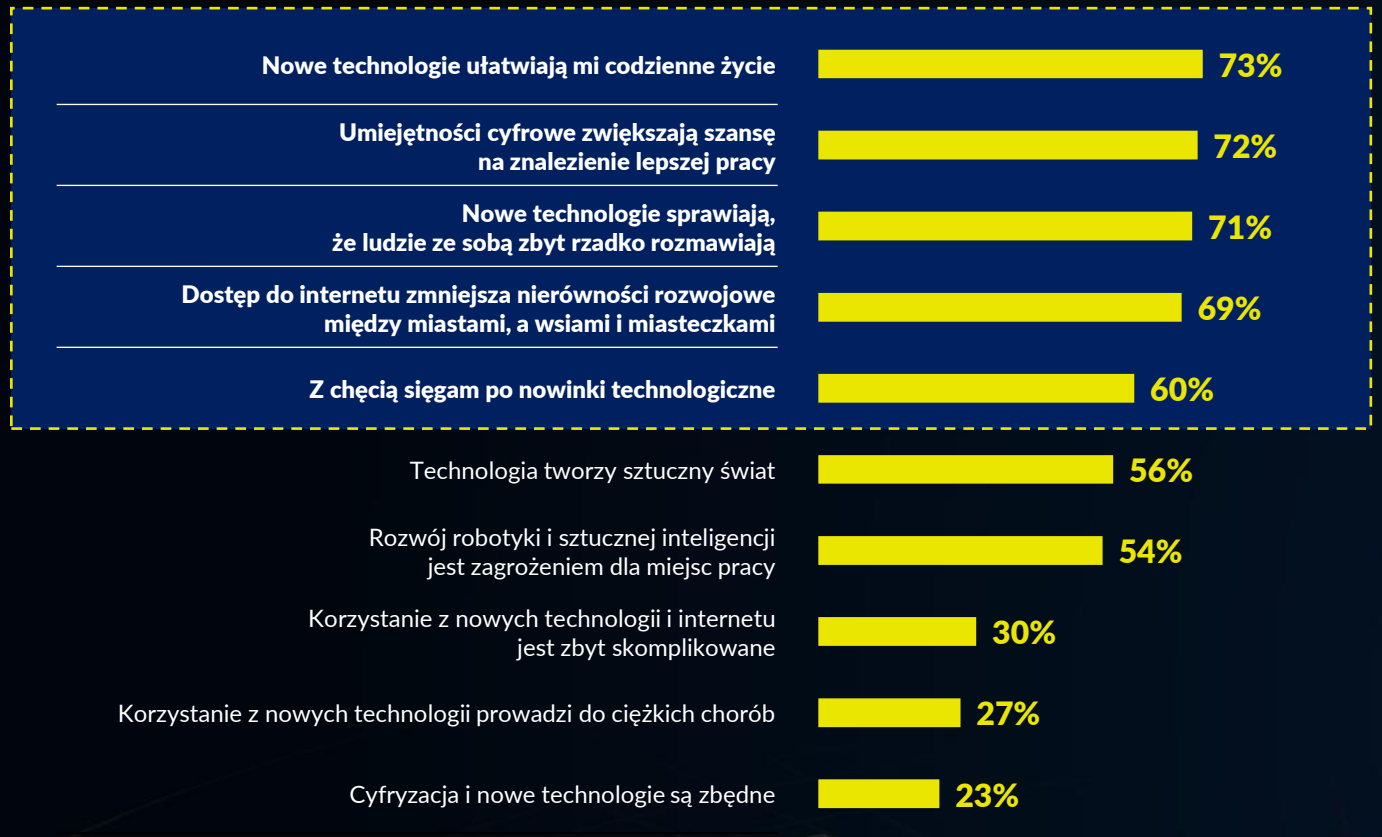
Jedną z głównych obaw w dalszym ciągu pozostaje wzrost cen. Choć w pierwszej połowie 2024 r. doświadczaliśmy najniższej od trzech lat inflacji, jej dotkliwe skutki pozostają w pamięci, prognozy zaś potwierdzają, że problemu tego będziemy w dalszym ciągu doświadczać choćby w przyszłym roku. Ogromnym wyzwaniem na przyszłość – tą nieco bardziej odległą – są postępujące zmiany demograficzne związane ze starzeniem się naszego społeczeństwa. Dobrze, że Polacy zauważają ten problem, jednocześnie coraz lepiej rozumiejąc jego konsekwencje. Znacznie zmalały na przykład obawy o bankructwo systemu emerytalnego, co nie jest realnym ryzykiem. Zagrożenie dotyczy raczej wysokości przyszłych świadczeń, możliwości zaspokojenia zapotrzebowania na opiekę zdrowotną czy też obciążeń podatkowych dla młodszych pokoleń.

Oddalają się na szczęście obawy związane z dezinformacją oraz polaryzacją. Rośnie jednak postrzeganie niedostatków w inwestycjach rozwój kompetencji pracowników. Wskazuje to na potrzebę jeszcze szybszej niż dotąd adaptacji do nowych technologii i rozwiązań związanych m.in. ze sztuczną inteligencją.

1.2.

Nastawienie do nowych technologii oraz technologiczny profil Polaków

Nastawienie do cyfryzacji i nowych technologii



Większość z nas **pozytywnie postrzega technologię,** jako dającą nowe możliwości.

Dla niecałych **30%** z nas korzystanie z technologii jest **trudne** lub prowadzi do **ciężkich chorób.**

71% społeczeństwa dostrzega **negatywny wpływ** cyfryzacji na **więzi społeczne** i pogorszenia relacji międzyludzkich.

Nadal utrzymują się obawy wobec **AI,** która w ocenie **55%** Polaków **może być zagrożeniem dla miejsc pracy.**

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni częściej deklarowali chęć sięgania po nowinki technologiczne (68 vs 53%), są bardziej przekonani o tym, że dostęp do internetu zmniejsza nierówności rozwojowe między miastami, a wsiami i miasteczkami (73 vs 64%) oraz częściej niż kobiety stwierdzają, że umiejętności cyfrowe zwiększają szansę na znalezienie lepszej pracy (77 vs 68%).

Kobiety z kolei częściej deklarowały, że nowe technologie sprawiają, że ludzie ze sobą zbyt rzadko rozmawiają (75 vs 66%), technologia tworzy sztuczny świat (59 vs 53%) czy że rozwój robotyki i sztucznej inteligencji jest zagrożeniem dla miejsc pracy (57 vs 51%).

WIEK

Starsze osoby, w wieku ponad 60 lat, znacząco częściej niż najmłodsi Polacy (18-29 lat), zgadzali się, że dostęp do internetu zmniejsza nierówności rozwojowe między miastami, a wsiami i miasteczkami (75 vs 56%) oraz to że, nowe technologie przyczyniają się do mniejszej chęci na rozmowy między ludźmi (80 vs 59%). To również osoby starsze częściej wskazywały, że nowe technologie ułatwiają im codzienne życie (77 vs 66%), czy że umiejętności cyfrowe zwiększają szansę na znalezienie lepszej pracy (75 vs 65%).

Natomiast najmłodsza grupa Polaków częściej przyznaje, że cyfryzacja i nowe technologie są zbędne (33 vs 10%) oraz, że korzystanie z nowych technologii prowadzi do ciężkich chorób (33 vs 13%).

Powyższe wyniki przeczą popularnym tezom jakoby to młodzi ludzi widzieli większe szanse w nowych technologiach czy aby to starsi bardziej obawiali się ciężkich chorób.

MIEJSCE ZAMIESZKANIA

Miejsce zamieszkania nie jest znaczącym wyróżnikiem w zakresie nastawienia do nowych technologii i cyfryzacji. Zmiany wynoszą najczęściej kilka punktów procentowych z wyjątkiem opinii o wyrównywaniu szans między miastami a wsiami dzięki użyciu technologii.

Mieszkańcy największych miast (powyżej 500 tyś. mieszkańców) trochę częściej niż mieszkańcy wsi przyznają, że internet zmniejsza nierówności rozwojowe między miastami, a wsiami i miasteczkami (79 vs 69%) oraz że nowe technologie ułatwiają im codzienne życie (80 vs 72%).

Z kolei mieszkańcy wsi częściej wskazywali, że cyfryzacja i nowe technologie są zbędne (22 vs 17%).

WYKSZTAŁCENIE

Wykształcenie jest nadal najważniejszym czynnikiem, który mocno różnicuje nastawienie do nowych technologii i cyfryzacji. Różnica w nastawieniu potrafi sięgać blisko 40 punktów procentowych.

Polacy z wyższym wykształceniem znacząco częściej niż posiadający podstawowe wykształcenie przyznają, że technologia ułatwia im codzienne życie (79 vs 41%), chętnie sięgają po nowinki technologiczne (66 vs 29%), umiejętności cyfrowe zwiększają szansę na znalezienie lepszej pracy (76 vs 55%) a internet zmniejsza nierówności rozwojowe między miastami a wsiami (77 vs 56%).

Osoby z podstawowym wykształceniem częściej zgadzają się, że rozwój robotyki i AI jest zagrożeniem dla miejsc pracy (63 vs 50%), cyfryzacja jest zbędna (29 vs 19%) a technologia tworzy sztuczny świat (58 vs 51%).

dr hab. Urszula Soler, prof. KUL

Katolicki Uniwersytet Lubelski Jana Pawła II

Tegoroczne badanie to kolejna, szósta już edycja niezwykle ważnego badania ukazującego stosunek Polaków do nowych technologii. Wciąż to mężczyźni chętniej niż kobiety sięgają po nowinki technologiczne (68 do 53%) i mniej się ich boją oraz uważają, że mogą poprawiać jakoś życia (77 do 69%). Kobiety częściej boją się tego, że nowe technologie oddalają ludzi od siebie (75 do 66%), tworzą sztuczny świat (59 do 53%) i są zagrożeniem dla miejsc pracy (57 do 51%). Na te obawy w dużym stopniu wpłynął z pewnością rozwój sztucznej inteligencji i dyskusje jakie wokół niego toczyły się w ostatnim roku.

Zaskakujące jest to, że nowe technologie najbardziej doceniają osoby 60+ (może to wynikać ze specyfiki badania – ankietę wypełniły tylko te osoby starsze, które faktycznie korzystają z technologii) – 77% – oraz osoby w średnim wieku (40–49 lat) – 76%. Najmniej doceniają je osoby najmłodsze (66%), co może świadczyć o tym, że nie do końca jeszcze rozumieją ich prawdziwe znaczenie, ponieważ w tej grupie wiekowej kojarzą się one głównie z rozrywką.

Co ciekawe, więcej osób w stosunku do ogółu Polaków w grupie wiekowej 30–39 lat uważa, że korzystanie z nowych technologii prowadzi do ciężkich chorób. Wartości te, co zaskakujące, są najniższe wśród osób najstarszych. Ponownie jednak ten wynik należałoby wiązać z innym sposobem przeprowadzenia badania, a tym samym doborem próby wśród osób najstarszych. Zauważalny jest także widoczny spadek (w stosunku do całej próby) w myśleniu, że nowe technologie są zbędne w tej oraz sąsiedniej grupie wiekowej. Wynik byłby bardzo optymistyczny, gdybyśmy mogli mieć pewność, że nie wynika on ze specyfiki metody badawczej.

Nie zaskakuje fakt, że najmniej chętnie, w stosunku do wszystkich Polaków, z nowych technologii korzystają osoby z wykształceniem podstawowym. Nie wpływają one ich zdaniem na możliwość znalezienia pracy. Co więcej, ich rozwój, zdaniem tej grupy, jest poważnym zagrożeniem dla ich zatrudnienia (63%). To także osoby z wykształceniem podstawowym oraz zasadniczym zawodowym najczęściej wskazują, że nowe technologie są zbędne.

Wyraźny wpływ na stosunek do nowych technologii widoczny jest w kategorii miejsce zamieszkania – z przewagą miast (szczególnie dużych) w stosunku do wsi. Bardzo ciekawe jest spostrzeżenie mieszkańców największych miast dotyczące tego, że nowe technologie zmniejszają nierówności rozwojowe pomiędzy miastami a wsiami i miasteczkami – uważa tak aż 79% badanych w tej grupie. Nieco mniej optymistyczni są mieszkańcy tych wsi i miasteczek, wśród których wartość ta nie przekracza 69%. Bardzo ciekawe w tej kategorii jest to, że mieszkańcy małych miasteczek uważają najczęściej, że korzystanie z nowych technologii prowadzi do ciężkich chorób (37% w tej grupie w stosunku do 22–26% w pozostałych).

Na podstawie wyników badań można było wśród badanych wyodrębnić pięć segmentów: entuzjaści (16%), realiści (22%), pragmatycy (26%), zdystansowani (17%) i ostrożni (19%). Pierwsze trzy grupy możemy określić jako te, które są pozytywnie nastawione do nowych technologii, chętnie z nich korzystają z różnych powodów (czasem widząc ich użyteczność) i są na nie otwarte. Oznacza to, że 64% Polaków ma stosunek pozytywny do nowych technologii. Czwartą grupą są zdystansowani – najczęściej mężczyźni w wieku 18–24 lat. Jest to grupa o tyle zaskakująca, że warto się nad nią bardziej pochylić. Są to osoby najrzadziej korzystające z internetu, częściej mieszkające na wsi. Sceptycznie podchodzą do nowych technologii, najmniej chętnie sięgają po nowinki technologiczne i nie widzą potencjału internetu w zmniejszeniu nierówności rozwojowych między miastami a wsią oraz nie widzą szans na znalezienie lepszej pracy dzięki posiadanym umiejętnościom cyfrowym. Są mało otwarci na korzystanie z różnorodnych nowoczesnych rozwiązań technologicznych. Jednocześnie zdają się nie dostrzegać, a nawet negują możliwe negatywne strony cyfryzacji i nowych technologii. Niezwykle istotny w tej grupie jest fakt, że należą do niej najmłodsi dorośli, o których przywykliśmy myśleć, że nowoczesne technologie od urodzenia były nieodłączną częścią ich życia. Być może winę za taki stan rzeczy ponosi brak edukacji technologicznej – młodzi ludzie, zwłaszcza na wsiach, nie wiedzą do czego technologii w sposób produktywny używać, bo do tej pory korzystali z niej tylko do rozrywki. Równocześnie ich dostęp do technologii jest mniejszy niż mieszkańców miast i brakuje im doświadczenia wynikającego z pracy zawodowej, w której nowe technologie odgrywają już często bardzo duże znaczenie. Ostatnią grupą są ostrożni – przede wszystkim starsze kobiety z podstawowym wykształceniem, o słabej sytuacji finansowej mieszkanki miast. Wyrażają one wiele obaw w związku z korzystaniem z nowych technologii i są najmniej na nie otwarte, wskazując także na to, że są one dla nich zbyt skomplikowane i szkodliwe dla zdrowia. Tu również pokutuje widoczny brak właściwej edukacji technologicznej w naszym społeczeństwie.

dr Michał Boni

Prezes fundacji Digital Poland, były Minister Cyfryzacji i Administracji, adiunkt na Uniwersytecie SWPS, Senior Researcher Associate w Martens Centre, Senator SME Europe, przewodniczący FISE (Fundacja Inicjatyw Społeczno-Ekonomicznych)

Mimo zawrotnej skali zmian cyfrowych przeszło 1/3 Polaków jest ostrożna albo ma dystans do nowych technologii. To w większości kobiety i osoby starsze oraz z podstawowym wykształceniem. Są oni mało otwarci na nowe rozwiązania technologiczne, obawiają się wyparcia z rynku pracy, niekoniecznie uważają, że nowe technologie ułatwiają życie codzienne na wielką skalę, czują, jak „internety" odbierają im realność i smak świata.

Entuzjastów jest 16%, a widać ich najczęściej wśród osób starszych (ceniących praktyczne funkcje urządzeń) oraz między 30. a 40. rokiem życia. Realistów jest więcej (22%) i generacyjnie są oni bardziej dojrzali, dostrzegają zarówno niebywałe szanse, jakie nowe technologie niosą, jak i zagrożenia – lęki o miejsca pracy, obawy przed zakłóceniem życia prywatnego i relacji społecznych.

O kierunku rozwoju postaw świadczą jednak najbardziej pragmatycy (26%): dostrzegają możliwości, jakie nowe technologie przynoszą na co dzień, w pracy, w życiu publicznym i chcą korzystać z coraz to nowych funkcjonalności, jakie one tworzą. Nie są obojętni na zagrożenia – mogą być ważnym, wiarygodnym społecznym partnerem działań i polityk publicznych uczących internetu i korzystania z niego w zrównoważony sposób. Widzą bowiem korzyści ekonomiczne i życiowe nowych technologii i chcieliby je mnożyć – taki wniosek wyciągnąłbym z analizy charakterystyki ich postawy.

To zresztą znakomita podstawa oraz sposób, by w ramach publicznej promocji nowych technologii razem z tą grupą przekonywać zdystansowanych – do wagi uczenia się nowych technologii i korzystania z nich dla dobra własnego oraz publicznego. Patrząc w przyszłość, przy niezbędnym dla rozwoju i zaawansowania technologicznego w Polsce – taki rodzaj polityki publicznej, wsparty działaniami edukacyjnymi, przygotowałby adaptacyjność społeczną na nowe wyzwania świata cyfrowego.

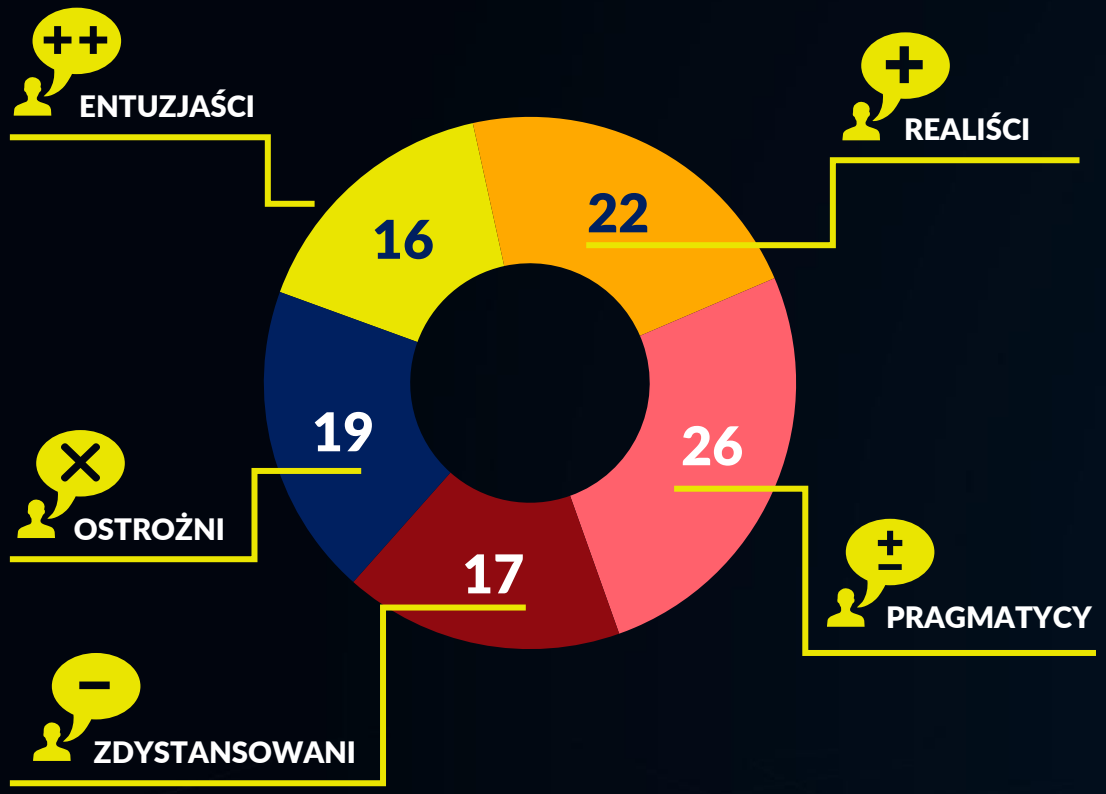
Z analizą poglądów Polaków na zmiany świata powiązany jest stosunek do roli, jaką nowe technologie odgrywają. Zostawiam na boku te oceny nowych technologii, które generują postawy dystansu (poniżej 30% wskazań), wynikają bowiem albo z niewiedzy, albo z przyjęcia za prawdziwe teorii spiskowych (technologie a ciężkie choroby).

Wśród pozostałych siedmiu głównych ocen natomiast trzy dotyczą obaw: że nowe technologie powodują, iż mniej rozmawiamy ze sobą (71%!) , że grożą naszej pozycji na rynku pracy (54%), że tworzą sztuczny świat, zmieniając tym samym nasze bycie w rzeczywistości (56%), a cztery oceny skupione są na szansach. Obawy, bardziej charakteryzujące kobiety, część osób starszych, nisko wykształconych i z małych miejscowości – muszą stać się przedmiotem troski polityki cyfryzacji. Ich neutralizacja jest ważnym czynnikiem rozwoju cyfrowego Polski.

Wśród cech pozytywnych, jakie niosą nowe technologie, oprócz ułatwiania życia, szans na lepszą, inną pracę dzięki rozwijanym umiejętnościom cyfrowym (72% – dobry znak dla edukacji na rzecz adaptacyjności), chęci powszechnego stosowania nowych rozwiązań (ważny sygnał mówiący o otwartości konsumenckiej Polaków na nowinki technologiczne), jest jeszcze przekonanie, że cyfrowe narzędzia mogą zmniejszać nierówności społeczno-terytorialne (miasto–wieś). Istnieje jednak spory rozdźwięk co do tej opinii pomiędzy mieszkańcami dużych miast a tymi, którzy żyją na wsi i w małych miasteczkach – ci ostatni są mniej pewni, czy ten mechanizm rzeczywiście działa.

Przedstawione badania można traktować jak kolejną fotografię zmian w polskim społeczeństwie, powiązanych z technologicznym boomem, z jakim mamy do czynienia w świecie. Ale ta fotografia mogłaby posłużyć też temu, by w oparciu o obraz i dane tworzyć polityki publiczne wspierające zaawansowanie cyfrowe Polski i Polaków. I otwierać poważną debatę, jakie cele – edukacyjne, promocyjne, świadomościowe – postawić!

Technologiczne profile Polaków 2024



Blisko **65% Polaków** jest nastawionych **pozytywnie** do nowych technologii.

17% z nas jest sceptykami,
a 19% podchodzi do niej ostrożnie.

Segmentacja technologicznych profili Polaków

Entuzjaści – 16%

Charakterystyka: częściej mężczyźni, trochę częściej osoby w wieku 30-49 jak i 60-75 lat, częściej z wykształceniem średnim lub wyższym, częściej z dużych miast, częściej w dobrej sytuacji ekonomicznej, częściej codziennie korzystający z internetu. Mają pozytywne nastawienie do nowych technologii. Chętnie z nich korzystają i chętnie sięgają po nowinki technologiczne. Widzą potencjał w zmniejszeniu nierówności rozwojowych między miastami a wsią poprzez dostęp do internetu jak też uważają, że umiejętności cyfrowe dają szanse na znalezienie lepszej pracy. Są najbardziej otwarci na korzystanie z różnorodnych nowoczesnych rozwiązań technologicznych.

Realiści – 22%

Charakterystyka: po równo kobiety i mężczyźni, trochę częściej osoby w wieku 40-49 lat, częściej z wykształceniem średnim, częściej z małych miast do 50 tyś, częściej codziennie korzystający z internetu. Podobnie jak „Entuzjaści" mają pozytywne nastawienie do nowych technologii. Chętnie z nich korzystają i chętnie sięgają po nowinki technologiczne. Widzą potencjał w zmniejszeniu nierówności rozwojowych między miastami a wsią poprzez dostęp do internetu jak też uważają, że umiejętności cyfrowe dają szanse na znalezienie lepszej pracy. Jednak dostrzegają też negatywne strony nowoczesnych technologii, takie jak: zmniejszenie kontaktów interpersonalnych, tworzenie sztucznego świata, zagrożenie dla miejsc pracy czy nawet zagrożenie dla zdrowia. Są otwarci na korzystanie z różnorodnych nowoczesnych rozwiązań technologicznych, jednak w trochę mniejszym stopniu niż „Entuzjaści".

Pragmatycy – 26%

Charakterystyka: trochę częściej mężczyźni, trochę częściej w wieku 50-59 lat, trochę rzadziej z wykształceniem podstawowym, trochę częściej ze wsi i małych miast do 50 tyś. Mają umiarkowanie mają pozytywne nastawienie do nowych technologii. Chętnie z nich korzystają i dość chętnie sięgają po nowinki technologiczne. Uważają, że umiejętności cyfrowe są szansą na znalezienie lepszej pracy. W umiarkowanym stopniu są otwarci na korzysta-nie z różnorodnych nowoczesnych rozwiązań technologicznych.

Zdystansowani – 17%

Charakterystyka: częściej mężczyźni, częściej w wieku 18-24 lata, najrzadziej korzystający z internetu, częściej mieszkający na wsi. Sceptycznie podchodzą do nowych technologii. Najmniej chętnie sięgają po nowinki technologiczne. Nie widzą potencjału internetu w zmniejszeniu nierówności rozwojowych między miastami a wsią. Ani nie widzą szans na znalezienie lepszej pracy dzięki posiadanym umiejętnościom cyfrowym. Jednocześnie zdają się nie dostrzegać czy też negują możliwe negatywne strony cyfryzacji i nowych technologii. Są mało otwarci na korzystanie z różnorodnych nowoczesnych rozwiązań technologicznych.

Ostrożni – 19%

Charakterystyka: najczęściej kobiety, częściej w wieku 60-75 lat, częściej z podstawowym wykształceniem (podstawowym lub zawodowym), częściej o słabej sytuacji ekonomicznej, trochę częściej mieszkający w miastach. Postrzegają nowe technologie jako tworzące sztuczny świat, jako zagrażające utrzymywaniu kontaktów interpersonalnych jak i stanowiące zagrożenie dla miejsc pracy. Jednocześnie na przeciętnym poziomie przyznają, że nowe technologię są zbyt skomplikowane czy szkodliwe dla zdrowia. Są najmniej otwarci na korzystanie z różnorodnych nowoczesnych rozwiązań technologicznych.

Anna Streżyńska

Główny doradca strategiczny KIGEiT, była Minister Cyfryzacji, Digital Shapers 2020

Podobnie jak w poprzednich latach nastawienie dwu grup: kobiet, zwłaszcza starszych oraz młodzieży do 24. roku życia kontrastuje z ogólnym poziomem akceptacji technologii cyfrowych. Kobiety są zarazem bardziej zdystansowane, jak i bardziej emocjonalne, jeśli chodzi o ocenę nowych technologii i związanych z nimi zagrożeń. To mocno koliduje z powszechnym przekonaniem, że kobiety są równie cyfrowe jak mężczyźni. Możemy tak mówić w odniesieniu do poszczególnych jednostek, lecz jako grupa we wszystkich badanych parametrach prezentują bardziej wstrzemięźliwe stanowisko i mniejszą gotowość cyfrową. Kobiety jako matki i nauczycielki rzadziej będą zatem wprowadzać młodzież w świat technologicznych nowinek.

W przypadku młodzieży zaskakujące jest to, że ci, o których mawiamy, że są cyfrowymi tubylcami, że urodzili się z komórką w ręce, w tak istotny statystycznie sposób kwestionują znaczenie i potrzebę technologii.

Pozostałe elementy charakterystyki: wykształcenie i miejsce zamieszkania, mogą dystans obu tych grup najwyżej wzmacniać. To lękowe w przypadku kobiet, a negatywne w przypadku młodzieży nastawienie jest już tak trwałe, że szkoda poświęcać mu więcej miejsca. Od lat komentuję ten sam element corocznego badania i nic się tu nie zmienia.

Czy zatem wykonaliśmy wszystko co trzeba, żeby zmienić przekonania tych dwu grup? A szczególnie grupy 18–24, bo ona właśnie dopiero wchodzi w życie. Częściowo te deficyty wyrównałaby odpowiednia praca, lecz w charakterystyce tej grupy czytamy: częściej mieszkający na wsi.

Istotne jest właściwe zdefiniowanie problemu, ponieważ zgodnie ze statystykami GUS 93,3% gospodarstw domowych ma szerokopasmowy internet, 100% czternastolatków ma telefon komórkowy, a w grupie 18–24 lat 80% korzysta z rozmów telefonicznych, prawie 90% z e-maila i ponad 90% z mediów społecznościowych. Czyli problemem nie jest brak dostępu, lecz brak przełożenia na korzyści. Działania bardziej użyteczne reprezentują w tej statystyce zakupy przez internet. Tylko 60% tej grupy wiekowej ich dokonuje, co pewnie się wiąże z rozporządzalnym dochodem. Młodzi ludzie zatem przypuszczalnie mają mniejszy entuzjazm dla zaawansowanych technologii, bo znają tylko najprostsze przejawy aktywności w sieci.

Z opisu grupy zdystansowanych można niestety wywieść, że stosunek do technologii jest efektem ich życiowej sytuacji i uwięzienia w życiowych determinantach. Nikt tej grupie 12 czy 18 lat temu nie pokazał ani w domu, ani w szkole, że nauka umiejętności cyfrowych jest ważna dla ich przyszłości i może otworzyć im jakieś możliwości. Dwanaście lat temu, gdy zaczynali edukację, zakończyliśmy dopiero etap uwalniania rynku telekomunikacyjnego z wieloletniego monopolu i przechodziliśmy z xDSL na pierwszy milion łączy światłowodowych, usług cyfrowych nie było, a wieś była spóźnionym beneficjentem zmian.

Grupa ta ze względu na całą swoją charakterystykę nie otrzymała być może ani wtedy, ani potem swojej szansy i prawdopodobnie boryka się dziś z o wiele bardziej istotnymi problemami niż kompetencje cyfrowe. Zachodzi pytanie o celowość naszej walki z wykluczeniem cyfrowym. Bo czy podniesienie kompetencji cyfrowych w tej grupach zmieni diametralnie ich życie bez jednoczesnego wykształcenia w nich determinacji i zdolności do znacznie dalej idącej życiowej zmiany?

1.3.

Chęć korzystania z nowych technologii odpowiadających na strategiczne wyzwania stojące przed Polską

Chęć skorzystania z nowych technologii

Najchętniej skorzystamy z rozwiązań ekologicznych i energii odnawialnej (70%).

Polacy popierają cyfryzację opieki zdrowotnej. Chcemy np. kupić antybiotyki przez internet (56%) czy udostępnić anonimowo swoje dane medyczne do badań (55%).

Ponad połowa Polaków chciałaby móc załatwiać sprawy urzędowe online (54%) czy skorzystać z samochodu elektrycznego (52%).

Rzadziej (30%) chcemy skorzystać z rozwiązań AI, które radykalnie zmieniają nasz sposób funkcjonowania. Na końcu rankingu znajdują się takie rozwiązania jak roboty opiekujące się starszymi osobami (26. miejsce) czy dokonujące operacji w szpitalu (23. miejsce). Konsumenci są stosunkowo ostrożni wobec technologii ingerujących w ciało lub zdrowie (45%).

4 na 10 Polaków chce skorzystać z innowacyjnych metod płatności dokonywanych za pomocą odcisku palca czy twarzy. Co czwarty Polak jest otwarty na kryptowaluty.

Ranking gotowości do skorzystania z nowych rozwiązań

	Procent Polaków chcących skorzystać z rozwiązania	RANKING	Różnica w rankingu vs 2023
Produkty uzyskane z recyklingu	72	1	0 =
Powszechnie instalowane wiatraki generujące czysty prąd	66	2	0 =
Panele słoneczne instalowane na dachach każdego domu, celem produkcji czystego prądu	60	3	0 =
Korzystanie ze smartfona / tabletu do nauki w szkołach/ na uniwersytetach	59	4	/brak w 2023/
Inteligentny dom - czujniki energii czy jakości powietrza oraz aplikacje automatyzujące działanie	56	5	+1 ↑
Antybiotyki i leki na receptę dostępne przez Internet	56	6	+10 ↑
Udostępnianie instytucjom naukowym swoich anonimowych wyników badań medycznych w celu stworzenia nowych metod leczenia wybranych chorób	55	7	-3 ↓
Załatwianie wszystkich spraw urzędowych i administracyjnych cyfrowo i całkowicie zrezygnowanie z tradycyjnej i papierowej formy komunikacji	54	8	+5 ↑
Podróż samochodem na prąd lub wodór	52	9	-4 ↓
Noszenie specjalnych opasek monitorujących stan zdrowia i przesyłających informacje do lekarza	52	10	-1 ↓
Zamontowanie w pobliżu Twojego domu małych anten, które pozwolą korzystać z nowej sieci komórkowej	52	11	-1 ↓
Głosowanie w wyborach (np. do sejmu, prezydenckich) przez Internet	52	12	+3 ↑
Prąd z elektrowni atomowej wybudowanej w Twoim województwie	51	13	-6 ↓
Asystent AI (program komputerowy) w pracy, nauce, który zwiększy Twoją produktywność lub uzyskasz dzięki niemu więcej czasu wolnego	51	14	-6 ↓
Sklep bez obsługi - samemu trzeba zeskanować wybrane produkty, a przy wyjściu sklep sam pobiera opłatę z konta	51	15	-1 ↓
Konsultacja u lekarza przez Internet – za pomocą kamery video	50	16	+3 ↑
Dostarczenie zakupów i przesyłek przez roboty, w tym drony	49	17	0 =
Wymiana organów (np. wątroba) na nowe, które zostały wydrukowane lub wychodowane	46	18	-7 ↓
Jedzenie uzyskiwane z inteligentnych i zielonych farmy, na których pracują roboty np. autonomiczne traktory oraz drony	45	19	+1 ↑
Zawarcie umowy na zakup nieruchomości, ziemi czy samochodu w formie elektronicznej umowy opatrzonej podpisem kwalifikowanym	45	20	/brak w 2023/
Sztuczna inteligencja analizująca braki w umiejętnościach cyfrowych i tworząca indywidualny program ich rozwoju	43	21	-3 ↓
Płacenie za pomocą odcisku palca lub weryfikacji twarzy	40	22	-1 ↓
Operacja (np. wycięcie wyrostka robaczkowego) dokonywana przez robota, a nie chirurga	33	23	+1 ↑
Podróż autobusem, w którym nie ma kierowcy, bo autobus jest kierowany przez komputer	32	24	+2 ↑
Diagnoza medyczna, jak np. wynik badania USG, postawiona przez sztuczną inteligencję, zamiast tradycyjnego lekarza	31	25	+3 ↑
Roboty opiekujące się starszymi osobami	30	26	-1 ↓
Zastępowanie produktów mięsnych przez zbliżone smakiem i właściwościami zamienniki roślinne i owady	29	27	+2 ↑
Sztuczna inteligencja wydająca wyroki sądowe w prostych sprawach jak np. mandat za przekroczenie prędkości	28	28	-1 ↓
Otrzymanie wynagrodzenia, świadczenia lub emerytury w kryptowalucie np. bitcoin, ethereum	23	29	/brak w 2023/

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni bardziej niż kobiety są otwarci na skorzystanie z nowoczesnych rozwiązań. Największe różnice dotyczą następujących rozwiązań: korzystanie z prądu z elektrowni atomowej zlokalizowanej w województwie, w którym się mieszka (61 vs 41%), wymiana organów (np. wątroba) na nowe, które zostały wydrukowane lub wychodowane (56 vs 37%), podróżowanie pojazdem autonomicznym (41 vs 23%), podróż samochodem na prąd lub wodór (60 vs 43%), załatwianie wszystkich spraw urzędowych i administracyjnych cyfrowo (63 vs 46%), korzystanie ze smartfona, tabletu do nauki w szkołach/ na uniwersytetach (68 vs 52%), korzystanie ze sklepu bez obsługi (59 vs 43%), dostarczenie zakupów i przesyłek przez roboty, drony (57 vs 41%) oraz korzystanie z indywidualnego programu stworzonego przez AI w celu analizy braków w umiejętnościach cyfrowych (50 vs 36%).

WIEK

Najmłodsi Polacy (w wieku 18-24) znacząco częściej niż najstarsze osoby (w wieku 60+) są skłonni skorzystać z nowych technologii takich jak: otrzymanie wynagrodzenia w kryptowalucie (36 vs 9%), zastępowanie produktów mięsnych przez zamienniki roślinne i owady (41 vs 18%), podróżowanie autonomicznym autobusem (38 vs 21%), korzystanie ze sklepu bez obsługi (61 vs 45%), dostarczenie zakupów i przesyłek przez roboty, drony (56 vs 40%) oraz udostępnianie instytucjom naukowym swoich anonimowych wyników badań medycznych w celu stworzenia nowych metod leczenia chorób (57 vs 44%), dostępność przez internet antybiotyków i leków na receptę (57 vs 45%).

Z kolei najstarsze osoby znacząco częściej niż najmłodsi Polacy są otwarci na rozwiązania ekologiczne jak: produkty uzyskane z recyklingu (77 vs 57%), panele słoneczne na dachach domów do produkcji czystego prądu (59 vs 47%) czy podróżo-wanie samochodem na prąd lub wodór (53 vs 45%).

MIEJSCE ZAMIESZKANIA

Mieszkańcy największych miast (powyżej 500 tyś. mieszkańców) częściej niż mieszkańcy wsi są bardziej otwarci na głosowanie w wyborach przez internet (67 vs 47%), panele słoneczne na dachach domów do produkcji czystego prądu (75 vs 58%), dostępność przez internet antybiotyków i leków na receptę (66 vs 51%), konsultacja u lekarza przez internet (61 vs 46%), załatwianie wszystkich spraw urzędowych i administracyjnych cyfrowo (63 vs 51%), zawieranie umów na zakup nieruchomości, ziemi czy samochodu w formie elektronicznej z podpisem kwalifikowanym (55 vs 43%).

Nie zaobserwowano różnic w przypadku chęci otrzymywania wynagrodzenia, świadczenia lub emerytury w kryptowalucie np. bitcoin, ethereum, jak również operacji (np. wycięcie wyrostka robaczkowego) dokonywanej przez robota, a nie chirurga oraz w przypadku sztucznej inteligencji wydającej wyroki sądowew prostych sprawach jak np. mandat za przekroczenie.

WYKSZTAŁCENIE

Wykształcenie jest najważniejszym czynnikiem, który mocno różnicuje chęć skorzystania z nowych technologii – różnice w nastawieniu wynoszą nawet 33 punkty procentowe. Szczególnie jest to widoczne w odniesieniu do: głosowania w wyborach przez internet (63 vs 30%), korzystania z indywidualnego programu stworzonego przez AI w celu analizy braków w umiejętnościach cyfrowych (54 vs 24%), wymiany organów (np. wątroba) na nowe, które zostały wydrukowane lub wychodowane (56 vs 27%), używania produktów z recyklingu (79 vs 50%), korzystania ze smartfona/ tabletu do nauki w szkołach/ na uniwersytetach (63 vs 35%), dostępności przez internet antybiotyków i leków na receptę (64 vs 36%) oraz korzystania z prądu z elektrowni atomowej zlokalizowanej w województwie, w którym się mieszka (56 vs 31%).

Ksawery Stojak

Menedżer Zespołu Transformacji Cyfrowej Przedsiębiorstw, Bank Gospodarstwa Krajowego

Polacy najchętniej wykorzystaliby technologie w ochronie zdrowia – tak wynika z raportu. Spośród ośmiu wymienionych technologii w tym obszarze, największym zainteresowaniem cieszy się możliwość zakupu antybiotyków i leków na receptę online (56%). Ponad połowa respondentów byłaby gotowa udostępnić zanonimizowane dane medyczne instytucjom naukowym (55%) i przesyłać dane z opasek monitorujących do lekarzy (52%). Znaczna część z nich zaakceptowałaby konsultację z lekarzem online (50%) oraz wymiany narządów na sztuczne (46%). Mniejsze zainteresowanie dotyczyło robotów do operacji i opieki nad osobami starszymi (30%). Rosnąca świadomość zdrowotna, wydłużony czas oczekiwania w szpitalach oraz wyzwania demograficzne, takie jak starzenie się społeczeństwa, przyczyniają się do zwiększonego zapotrzebowania na efektywniejszą opiekę zdrowotną. Pandemia wirusa SARS-CoV-2 również mogła być ważnym czynnikiem w zwiększeniu się społecznej akceptacji rozwiązań telemedycznych.

Duże zainteresowanie Polaków dotyczy też technologii odnawialnych źródeł energii (OZE) i produktów z recyklingu (72%). Szczególnie popularne są instalacje turbin wiatrowych (66%) i paneli słonecznych (62%). Ponad połowa respondentów chciałaby korzystać z samochodów elektrycznych lub wodorowych (52%) oraz energii jądrowej (51%). Kryzys energetyczny, wywołany m.in. wojną w Ukrainie, mógł wpłynąć na te postawy. W efekcie zmniejszenie kosztów energii oraz niezależność od zewnętrznych dostawców stają się kluczowe.

W obszarze cyfryzacji Polacy oczekują dalszego rozwoju już dostępnych technologii. Cyfrowe załatwianie spraw urzędowych (54%), głosowanie online (52%) oraz tablety w szkołach (59%) są istotnymi oczekiwaniami. Cyfryzacja zmniejsza zużycie papieru i ogranicza emisję CO_2, a także wpływa na poprawę efektywności energetycznej domów, na przykład przez czujniki jakości powietrza i energii (56%). Zmniejsza się też obawa przed technologią 5G (52%).

Bank Gospodarstwa Krajowego (BGK) odgrywa ważną rolę w finansowaniu innowacji. Poprzez dystrybucję środków z Krajowego Planu Odbudowy (KPO), BGK wspiera transformację cyfrową, energetyczną oraz zieloną transformację miast. Ważnym projektem jest DigSus, który minimalizuje negatywne skutki cyfryzacji, promując technologie o pozytywnym wpływie społecznym.

Z wyjątkiem produktów uzyskanych z recyklingu, kobiety rzadziej korzystają z nowych technologii, co wskazuje na potrzebę wsparcia ich kompetencji cyfrowych. Przez projekt **GoDigital**, BGK wspiera rozwój tych kompetencji wśród kobiet przedsiębiorczyń. Największe zainteresowanie technologiami wykazuje grupa wiekowa 30-59 lat, a wysokie wykształcenie i zamieszkanie w miastach wpływają na otwartość na nowe rozwiązania.

Polacy coraz chętniej sięgają po nowe technologie, szczególnie w obszarze ochrony zdrowia, energii i cyfryzacji usług publicznych, rośnie także ich świadomość ekologiczna oraz potrzeba automatyzacji i efektywności energetycznej. BGK, dzięki środkom z KPO oraz projektom takim jak DigSus i GoDigital, wspiera transformację cyfrową, energetyczną i zrównoważony rozwój, odpowiadając na te potrzeby.

dr Konrad Maj

Kierownik Centrum Innowacji Społecznych, Technologicznych HUMANTECH, Uniwersytet SWPS w Warszawie

Wyniki badania w zakresie otwartości Polaków na technologie pokazują, że ta otwartość z biegiem lat nieco spada. Zwłaszcza jeśli chodzi o takie rozwiązania technologiczne jak wymiana własnych organów na nowe, prąd z elektrowni atomowej czy korzystania z asystentów AI.

Wciąż jednak cenione są u nas rozwiązania, które mają potencjał poprawy jakości życia i zmniejszenia negatywnego wpływu na środowisko. Na pierwszych miejscach w rankingu popularności znalazły się niezmiennie produkty uzyskane z recyklingu (72%), instalowanie wiatraków generujących czysty prąd (66%) oraz panele słoneczne na dachach każdego domu (60%). Można to tłumaczyć rosnącą świadomością ekologiczną i potrzebą wprowadzania zrównoważonych rozwiązań, które są postrzegane jako odpowiedź na globalne wyzwania związane ze zmianami klimatu. Trudny jednak do interpretacji wydaje się być wzrost akceptacji dla antybiotyków i leków na receptę dostępnych przez internet w stosunku do poprzedniego badania (o 10 punktów). Być może jednak jest to kwestia ujęcia obu tych elementów w jednej kategorii, a za ten wzrost odpowiada coraz częstsze dokonywanie zakupu farmaceutyków przez internet, a nie większa popularność antybiotyków wśród Polaków.

Kolejne technologie, które zyskały dużą aprobatę, to inteligentne domy (56%) oraz możliwość załatwiania spraw urzędowych całkowicie cyfrowo (54%). To sugeruje, że Polacy poszukują technologii, które mogą zwiększyć komfort życia codziennego, zmniejszyć jego złożoność i oszczędzić czas.

Warto jednak zauważyć, że chociaż niektóre technologie spotkały się z entuzjazmem, to inne, bardziej zaawansowane rozwiązania budzą pewne obawy. Na przykład technologie związane z ingerencją w ciało ludzkie. Takie rozwiązania jak wymiana organów na wydrukowane lub hodowane (tylko 31% otwartych na skorzystanie) czy operacje przeprowadzane przez roboty (33%) cieszą się znacznie mniejszą popularnością. Wynika to prawdopodobnie z obaw o bezpieczeństwo, niepewności co do skuteczności oraz braku zaufania do nowoczesnych technologii w medycynie. Można to interpretować również jako wyraz lęku przed nieznanym, a także opór przed naruszeniem granic osobistych przez technologię, która może być postrzegana jako „nieludzka". Być może prowokuje to pytania natury egzystencjalnej i etycznej odnoszące się do tego, do jakiego stopnia można ingerować w ludzki organizm i dokąd nas to może zaprowadzić.

Raport pokazuje, że młodsze osoby (19–29 lat) wcale nie są entuzjastami wielu innowacji technologicznych, ale za takich można uznać osoby w wieku 40–49 lat. Ten sceptycyzm może wynikać zarówno z niskiej wiedzy w tym zakresie, jak i wręcz odwrotnie – ze świadomości tego, że produkty z recyklingu to często efekt marketingowy. Z kolei starsze grupy wiekowe (60 lat i więcej) są bardziej sceptyczne wobec wielu nowinek technologicznych, szczególnie tych, które mogą wymagać znacznego dostosowania się lub nauki nowych umiejętności.

Podobnie osoby z wyższym wykształceniem w porównaniu do osób z podstawowym wykształceniem są ewidentnie bardziej skłonne do korzystania z zaawansowanych technologii, co może wynikać z większej świadomości korzyści, jakie te technologie oferują w określonym kontekście (np. wykorzystywanie smartfonów do wspierania edukacji na uniwersytetach), a także z większej pewności siebie w ich obsłudze (głosowanie w wyborach z wykorzystaniem technologii).

Chociaż wiele technologii spotyka się z akceptacją, niektóre propozycje, takie jak sztuczna inteligencja wydająca wyroki sądowe (23% akceptacji) czy operacje przeprowadzane przez roboty (33%), są wyraźnie odrzucane przez większość respondentów. Wynika to zapewne z obserwowanego w wielu badaniach niskiego poziomu zaufania społecznego do decyzji podejmowanych przez maszyny, obawy przed błędami technologicznymi oraz przekonania, że ludzki element jest niezbędny w procesach decyzyjnych gdzie rolę grają wartości, wrażliwość społeczna czy empatia.

Ogólnie analiza wyników raportu wskazuje na duże zróżnicowanie postaw Polaków wobec nowych technologii i też, że te postawy nie są stałe na przestrzeni lat. Wskazuje to wielką rolę edukacji, które może pokazywać szansę i zagrożenia związane z wykorzystaniem danej technologii, ale w oparciu o rzetelne badania naukowe i analizy, demaskując różne społeczne mity i doniesienia medialne.

dr hab. Agnieszka Skala, prof. PW

Kierownik Zakładu Przedsiębiorczości i Innowacji,
Wydział Zarządzania, Politechnika Warszawska

Środowisko (recykling, redukcja spalin), energia („czysty prąd" oraz optymalizacja jego zużycia), zdrowie (auto-monitoring, udostępnianie danych medycznych) i produktywność (pracy i czasu) to obszary, w których otwartość Polaków na nowe technologie jest największa.

Najbardziej spektakularny „awans" w rankingu akceptacji technologii zalicza właśnie energetyka atomowa, która z zagrożenia staje się sprzymierzeńcem prawie tak szybko, jak rosną nasze rachunki za prąd.

Z kolei znaczne spadki chęci Polaków do skorzystania zaliczają technologie takie jak zautomatyzowane zielone farmy, systemy rozpoznające twarze lub samochody oraz sztuczne mięso, przy czym tylko w ostatnim przypadku określiłabym tę chęć jako naprawdę niską (24%).

Moim zdaniem ranking kolejny raz pokazuje, że przede wszystkim unikamy tych technologii, których nie znamy albo nie rozumiemy ich działania lub potencjalnych skutków. To, co faktycznie wchodzi do użycia i zyskuje na powszechności lub przynajmniej staje się przedmiotem realnej debaty publicznej i wypowiedzi ekspertów, przestaje, szybciej lub wolniej, budzić lęki i obawy. Technologie z dolnych partii rankingu są wciąż w zalążku lub mało upowszechnione: robotyzacja, autonomizacja, wirtualna rzeczywistość. Potężnym motywatorem dla nowych rozwiązań jest też stan naszego portfela, który może przekonać nawet najbardziej opornych przeciwników atomu, zdalnej komunikacji czy cyfryzacji.

Jaki z tego wniosek? Edukacja i popularyzacja wiedzy – to najlepszy sposób na zwiększenie akceptacji dla wdrożeń nowych technologii. Wymiana dobrych praktyk, promocja sieci współpracy, otwarcie i popularyzacja nauki i wreszcie najważniejsze – formy i narzędzia nauczania oraz treści edukacyjne w szkołach i na uczelniach to główne kanały dotarcia z komunikatem o możliwościach (i zagrożeniach), jakie niosą nowe technologie. Powszechne i dostępne programy edukacyjne (mam na myśli: dla firm, instytucji, domów kultury, kółek seniorów, ośrodków i stowarzyszeń itp.) obiektywnie tłumaczące działanie, korzyści i zagrożenia z zastosowania nowych technologii to realne narzędzie wpływu na poziom otwartości na innowacje w naszym kraju i finalnie tworzące popyt wewnętrzny na te rozwiązania.

Ignacy Święcicki

Kierownik Zespołu Gospodarki Cyfrowej, Polski Instytut Ekonomiczny

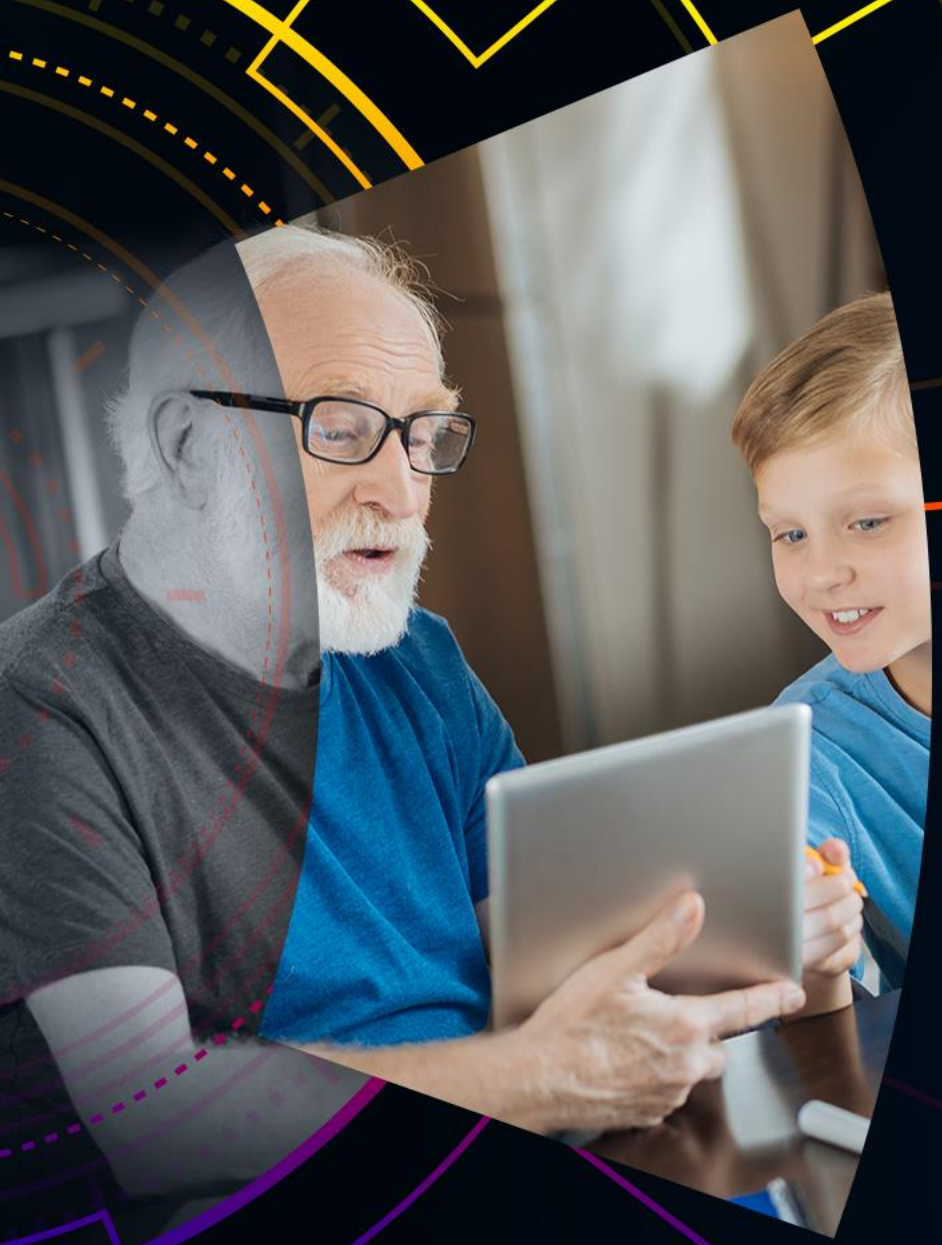
Czołówka rankingu nowych technologii pozostała w tym roku bez zmian – podium zajmują technologie związane z ochroną klimatu, a także dość długo obecne i niejako zadomowione w świadomości obywateli. Tak wysoka pozycja technologii klimatycznych podkreśla wagę wyzwań na styku energetyki i technologii cyfrowych – szerokie zastosowanie rozproszonych źródeł energii nie będzie efektywne bez cyfryzacji systemu i algorytmów pozwalających zarządzać dostępną mocą. W tym sensie wyniki badania wpisują się w narrację o bliźniaczej transformacji, jednoczesnej zmianie modeli energetycznych i cyfryzacji gospodarki.

Z kolei spojrzenie na drugą stronę tabeli pokazuje, jak niski jest poziom akceptacji dla decyzji podejmowanych bez udziału człowieka czy też przekazania maszynom lub AI całych procesów. Operacje wykonywane przez roboty czy podróż autobusem bez kierowcy znalazły akceptację tylko jednej trzeciej respondentów, a robotyczna opieka nad osobami starszymi czy propozycja wydawania wyroków przez AI (co mogłoby przecież w znacznej mierze odciążyć system sądowniczy i korzystnie wpłynąć na inne obszary) uzyskały jeszcze niższy odsetek wskazań. Na takie zmiany w społeczeństwie wyraźnie nie jesteśmy gotowi – a wynik ten utrzymuje się od lat w badaniach społeczeństwa 5.0.

Wydaje się również, że zwiększona ilość informacji i dyskusji o AI obecna w mediach od dwóch lat nie zmieniła w tym względzie opinii Polek i Polaków. Efekt może mieć natomiast nurt dyskusji wokół higieny cyfrowej oraz zagrożeń, jakie niesie ze sobą stałe korzystanie z urządzeń mobilnych. W tym kontekście zwraca uwagę chociażby spadek pozycji Asystenta AI – znacznie chętniej akceptowanej technologii w poprzednich edycjach badania. Mimo że jest to stosunkowo mało rewolucyjna technologia, spadła w rankingu aż o sześć miejsc.

Tradycyjnie wyższy poziom akceptacji dla nowych technologii wśród mężczyzn i osób wyżej wykształconych nie dziwi. Tym jednak, co zwraca uwagę (zresztą jest to zjawisko widoczne i w poprzednich edycjach raportu), jest otwartość na nowe technologie wśród osób w średnim wieku i starszych – w kilku przypadkach wyraźnie przekraczająca nastawienie osób z najmłodszych grup wiekowych. Biorąc pod uwagę wyniki innych badań, w tym chociażby dotyczących kompetencji cyfrowych, w których te grupy wypadają znacząco słabiej, jest to sygnał pozwalający z nadzieją patrzeć na pozytywne wykorzystanie technologii dla poprawy jakości naszego życia.

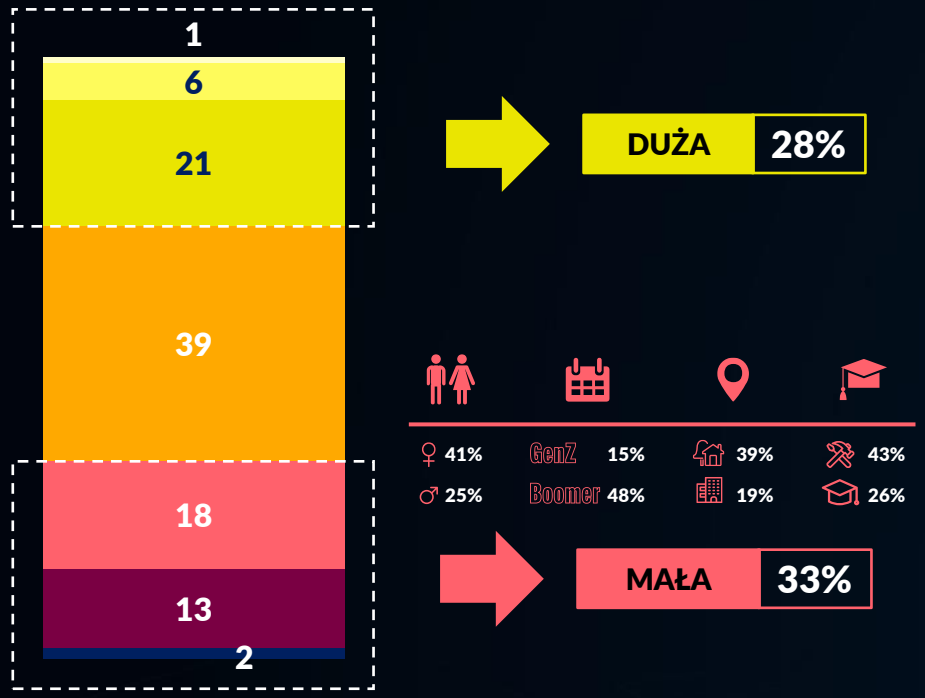
2. CYBERBEZPIECZEŃSTWO OCZAMI POLAKÓW 2024



2.1.

Jaką mamy wiedzę na temat cyberbezpieczeństwa?

Wiedza Polaków na temat cyberbezpieczeństwa



33% Polaków ma małą wiedzę na temat cyberbezpieczeństwa.

Tylko **3 na 10 Polaków** ocenia swoją wiedzę jako **dużą.**

Jestem ekspertem
Jest zdecydowanie duża
Jest raczej duża
Jest taka sobie / umiarkowana
Jest raczej mała
Jest zdecydowanie mała
Jest zerowa / żadna

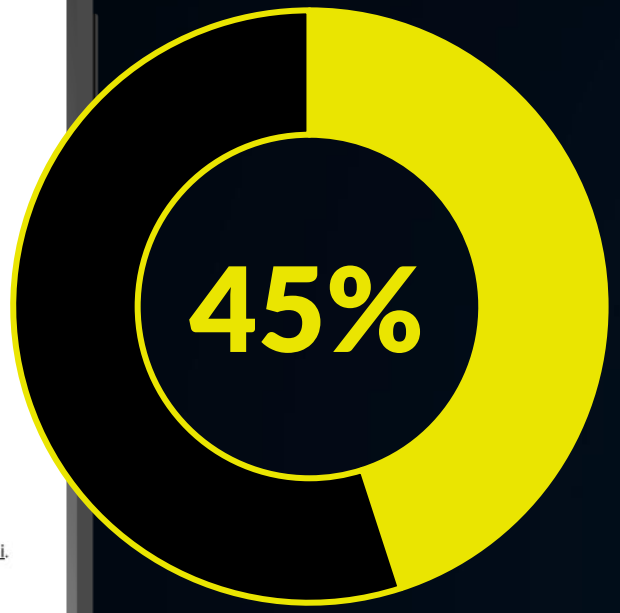
Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

dr Łukasz Olejnik, LL.M.

Niezależny badacz i konsultant, prowadzi bloga prywatnik.pl, związany z Department of War Studies King's College London, autor książek *Filozofia Cyberbezpieczeństwa* (PWN, 2022) i *Propaganda* (PWN, 2024)

Na podstawie wyników badań społecznych dotyczących świadomości cyberbezpieczeństwa w Polsce widać kilka wyróżniających się elementów. Większość badanych ocenia swoją wiedzę na temat cyberbezpieczeństwa jako umiarkowaną, a 66% z nich deklaruje chęć poszerzenia tej wiedzy. To bardzo chwalebne, zwłaszcza w kontekście tego, że 53% respondentów przyznaje, iż nie są pewni, czy ich urządzenia i konta są faktycznie bezpieczne. Jest to dziś rozsądna obawa, bo skąd mogą o tym wiedzieć? W dodatku krajobraz IT i zalecenia cyberbezpieczeństwa ewoluują. Latami eksperci i szkoleniowcy zalecali, by hasło było takie-a-takie, składało się z tego-a-tego zestawu znaków oraz że należy je koniecznie regularnie zmieniać. Dziś sytuacja uległa zmianie, wiemy lepiej, zalecenia są inne i np. odradza się częstą zmianę hasła bez wyraźnej potrzeby. To może jednak prowadzić do dysonansu poznawczego u użytkowników: czy można ufać zaleceniom?

W przypadku cyberincydentu 41% osób zadeklarowało, że zgłosiłoby się na policję. Jest to zgodne ze zdrowym rozsądkiem, ale także wskazuje na potrzebę usprawnienia komunikacji między instytucjami takimi jak policja i banki. W szczególności młodzi ludzie (18–29 lat) rzadziej (28%) preferują kontakt z instytucjami finansowymi bezpośrednio, co sugeruje potrzebę lepszego dostosowania kanałów zgłoszeń dla tej grupy. Starsi użytkownicy natomiast (60–75 lat) mogą wykazywać się tutaj większą mądrością życiową, preferując bardziej bezpośredni kontakt.



Blisko połowa Polaków nie zdała naszego testu na temat phishingu.

Test z wiedzy o phishingu

Tylko jedna odpowiedź w badaniu była poprawna

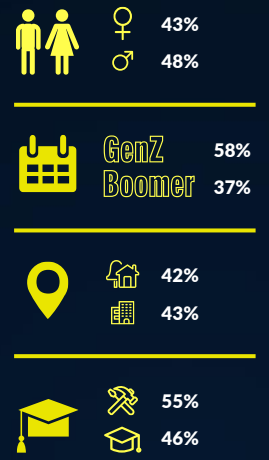
Nie wiem w ogóle czy e-mail przyszedł od Netflix. Może być prawdziwy lub fałszywy bo nie widzę adresu nadawcy e-mail. **55%**

To fałszywa wiadomość, należy ją zgłosić jako phishing/spam. **24%**

To poprawna wiadomość z serwisu Netflix. Wystarczy zrestartować hasło i po problemie. **16%**

Piotr ma np. wspólne konto z tatą, zapewne to on resetuje hasło. Piotr może mu pomóc klikając w link. **5%**

BŁĘDNE 45%



Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Izabela Taborowska

Wiceprezeska fundacji Girls in Tech, prezeska zarządu, CIO w CyberClue

Pomimo powszechności korzystania z Internetu i usług cyfrowych oraz wielu kampanii edukacyjnych w zakresie cyberbezpieczeństwa badanie pokazuje, jak wiele mamy jeszcze do zrobienia. 72% respondentów wskazało, że ma małą lub umiarkowaną wiedzę w tym zakresie. Jest to wynik przytłaczający. 28% respondentów określa swoją wiedzę jako dużą, co jest dobrym startem. Zdecydowanie niżej niż pozostałe grupy oceniają własne kompetencje w tym zakresie kobiety, osoby 50+ i te z wykształceniem podstawowym. Najlepiej oceniają się mężczyźni i osoby młodsze, w wieku 18–39 lat.

Stoi to częściowo w sprzeczności z wynikami ćwiczenia praktycznego. Fałszywego maila najlepiej rozpoznawały osoby w wieku 40–49, a zdecydowanie najgorzej wypadła grupa 18–29-latków, w której aż 58% błędnie zidentyfikowało phishing. Osoby mieszkające na wsi i w małych miast i z wykształceniem podstawowym miały najsłabsze wyniki. Ogólny wynik tego testu jest alarmujący – tylko 55% rozpoznało poprawie wiadomość e-mail. Jest to szczególnie ważne, biorąc pod uwagę, że około 75% ataków hackerskich zaczyna się w Polsce od maila phishingowego, a większość z nich kierowana jest masowo do dużej grupy przypadkowych użytkowników.

Cieszy, że 66% respondentów chętnie poszerzyłoby swoją wiedzę w zakresie cyberbezpieczeństwa. Chęć ta rośnie wraz z poziomem wykształcenia, niewiele się natomiast różni w zależności od wielkości miejscowości zamieszkania.

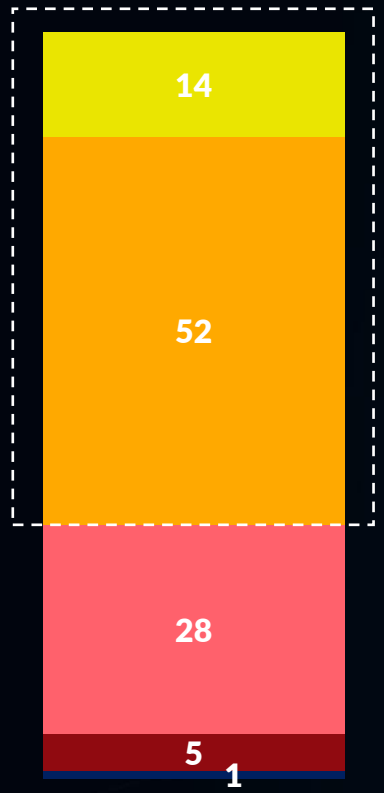
Proces postępowania w przypadku cyberataku nawet w najbardziej świadomej grupie (mężczyzn i 18–29-latków) zna tylko ok. 30%. Młodzi są bardziej skłonni do próby samodzielnego rozwiązania problemu, co nie dziwi, bo obcują z technologią na co dzień. Osoby z wyższym wykształceniem chętnie zwrócą się do znajomego posiadającego wiedzę IT. Respondenci z wykształceniem podstawowym jako najczęstszy punkt kontaktowy podali z kolei dostawcę internetu, najprawdopodobniej ze względu na brak innych kontaktów w tym obszarze.

Cieszy, że odruchy mamy dobre. 41% respondentów zgłosiłoby atak do organów ścigania, 38% do banku (przy naruszenia konta), a 25% do służb państwowych takich jak CERT czy CESIRT. Oznacza to, że kampanie administracji w tym zakresie zaczynają coraz lepiej działać.

Badanie wskazało, że osoby 50+, kobiety, respondenci z mniejszych miejscowości i z podstawowym wykształceniem mają mniejszą świadomość i wiedzę z obszaru cyber. Ogólne wyniki nawet w pozostałych grupach nie mogą jednak zadowalać. Praca u podstaw, budowanie świadomości powinny być celem na najbliższy czas.

Chęć pogłębienia wiedzy

z zakresu zagrożeń i cyberbezpieczeństwa



TAK 66%

♀ 68%	GenZ 58%	67%	53%
♂ 63%	Boomer 71%	68%	71%

2 na 3 Polaków chce pogłębić swoją wiedzę z zakresu cyberbezpieczeństwa.

Zdecydowanie chętnie
Raczej chętnie
Ani chętnie, ani niechętnie
Raczej niechętnie
Zdecydowanie niechętnie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

dr Agnieszka Jankowska

Członkini zarządu fundacji Digital Poland ds. edukacji cyfrowej, dyrektorka ds. korporacyjnych i public affairs, T-Mobile Polska, przewodnicząca Rady ds. Cyfryzacji przy Ministerstwie Cyfryzacji

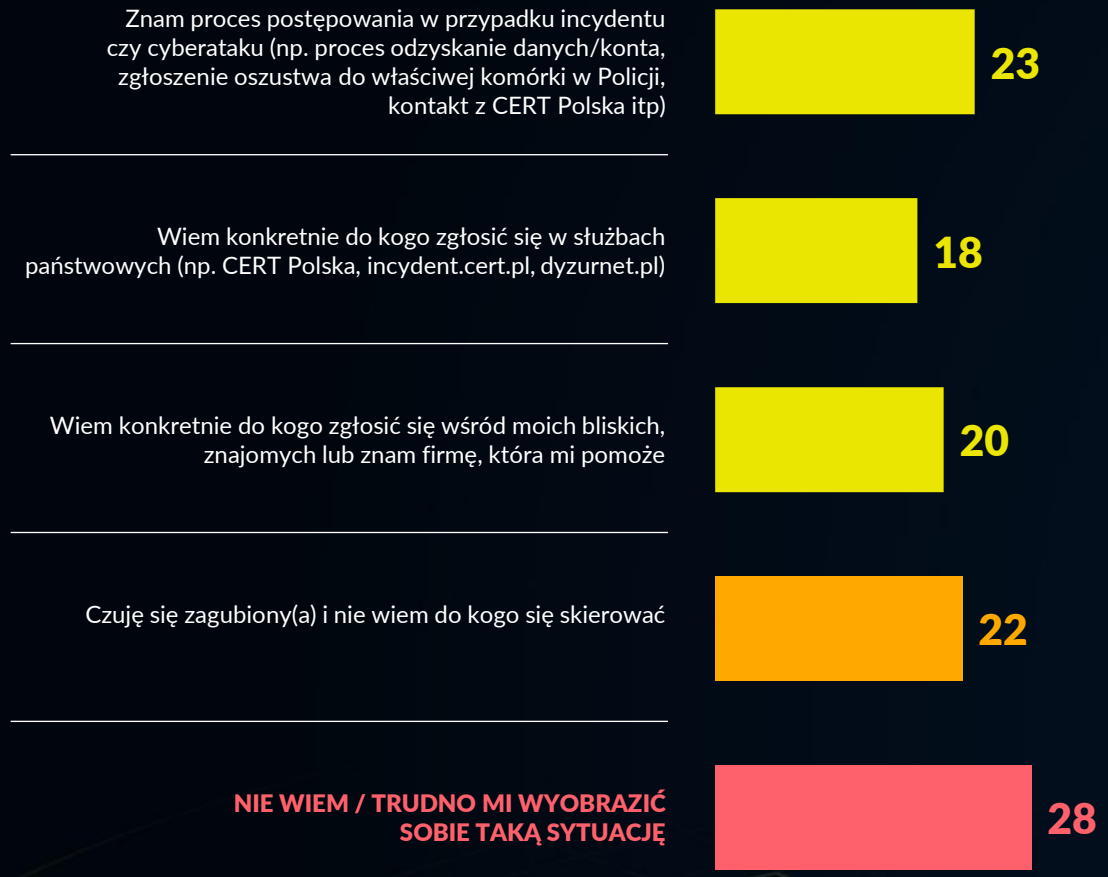
Cyberbezpieczeństwo stało się kluczowym aspektem współczesnego społeczeństwa i funkcjonowania w coraz bardziej cyfrowym świecie. Z roku na rok rośnie liczba zagrożeń, a użytkownicy internetu muszą stawiać czoła coraz bardziej wyrafinowanym formom cyberataków. Mimo że badania wskazują na to, że Polacy są coraz bardziej świadomi tych niebezpieczeństw, wciąż istnieją poważne luki zarówno w wiedzy naszych obywateli na temat zagrożeń, jak i w zakresie działań prewencyjnych.

Jednym z najbardziej alarmujących wyników niniejszego badania jest to, że aż 33% Polaków przyznaje się do małej lub zerowej wiedzy na temat cyberbezpieczeństwa, aczkolwiek zjawisko to jest częścią szerszego problemu, który dotyczy nie tylko Polski, lecz także wielu innych krajów europejskich. Z raportu Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) z 2023 roku wynika, że brak wiedzy na temat cyberzagrożeń jest jednym z kluczowych czynników zwiększających skuteczność cyberataków w całej Europie. Pomimo rosnącej świadomości (28% Polaków ocenia swoją wiedzę jako dużą) edukacja w zakresie cyberbezpieczeństwa nadal pozostaje niedostateczna, szczególnie w mniejszych miejscowościach oraz wśród starszych użytkowników internetu. W tym kontekście bardzo cieszy fakt, że blisko 66% Polaków deklaruje chęć pogłębienia swojej wiedzy o cyberzagrożeniach. To bardzo pozytywny sygnał, świadczący o tym, że Polacy dostrzegają znaczenie cyberbezpieczeństwa i są świadomi rosnących zagrożeń w internecie.

Wyniki badania wskazują, że Polacy posiadają zróżnicowany poziom wiedzy na temat sposobów reakcji na incydenty i cyberataki – tylko 23% badanych deklaruje znajomość procedur postępowania w przypadku cyberataku, 22% czułoby się zagubionych i nie wiedziałoby, co zrobić w takiej sytuacji, a dla 28% badanych taki scenariusz jest trudny do wyobrażenia. Wyniki te jednoznacznie wskazują na niedostateczne przygotowanie dużej części polskiego społeczeństwa na cyberzagrożenia, co w sytuacjach kryzysowych może prowadzić do opóźnień w prawidłowej reakcji oraz tym samym zwiększyć ryzyko utraty danych. Warto również zauważyć, że Polacy w przypadku ataków najczęściej zwróciliby się do lokalnych organów ścigania (42%) lub banków i instytucji finansowych (38%), co może świadczyć o większym zaufaniu do instytucji finansowych niż do służb państwowych, takich jak CERT Polska czy CSIRT NASK, które wybrałoby jedynie 25% ankietowanych.

Obawy Polaków dotyczące bezpieczeństwa w sieci, zwłaszcza te związane z kradzieżą tożsamości, zainstalowaniem złośliwego oprogramowania czy wyłudzeniem pieniędzy, są uzasadnione. Jak pokazują badania realizowane na poziomie unijnym, skala cyberataków rośnie. W 2022 roku zanotowano ponad 1,5 miliona incydentów z zakresu cyberbezpieczeństwa na terenie UE, co stanowi wzrost o 38% w porównaniu do poprzedniego roku. Co więcej, według danych ENISA aż 59% ataków skierowanych jest na osoby prywatne, a nie na organizacje, co wskazuje na to, że cyberprzestępcy coraz częściej wybierają indywidualnych użytkowników jako swoje cele. Nie dziwi zatem to, że niemal 2/3 Polaków wyraża obawy dotyczące bezpieczeństwa w sieci. Ponadto fakt, że aż 41% badanych uważa, że ryzyko stania się ofiarą ataku jest wysokie, pokazuje rosnącą świadomość zagrożeń, choć jednocześnie wskazuje na konieczność wprowadzenia bardziej efektywnych działań edukacyjnych w zakresie cyberbezpieczeństwa. Nadal istnieje wyraźna luka w wiedzy nie tylko na temat rodzajów zagrożeń internetowych, lecz także sposobów przeciwdziałania im, a w przypadku ich wystąpienia – odpowiedniej reakcji. Z tego względu konieczne jest podjęcie działań i akcji edukacyjnych kierowanych do szerokiego grona odbiorców, dedykowanych szkoleń dla różnych grup pracowników, w szczególności w sektorze publicznym, na poziomie regionalnym i lokalnym, jak również włączenie tematyki cyberbezpieczeństwa do systemu edukacji, tak aby uczennice i uczniowie już od najmłodszych lat byli zaznajamiani z problematyką zagrożeń w internecie, ochroną swoich danych, zabezpieczaniem urządzeń i postępowaniem w sytuacjach zagrożenia.

Wiedza na temat podstępowania w przypadku cyberataku lub incydentu



3 na 10 Polaków nie wie jak postąpić w przypadku cyberataku lub incydentu.

Co piąty czuje się zagubiony. Tylko ok. 25% zna procesy i wie do kogo się zgłosić.

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Do kogo udadzą się Polacy w razie cyberataku, oszustwa lub incydentu cyberbezpieczeństwa?

TOP 3

Rozpatrując hipotetyczną sytuację cyberataku, oszustwa czy incydentu **najwięcej** Polaków skierowałoby się **na Policję (41%) lub do instytucji finansowej (38%).** Jedynie **1 na 4 wybrałoby służby państwowe,** z kolei 20% skorzystałoby z pomocy rodziny lub znajomego.

Co dwudziesty Polak nic by nie zrobił w przypadku cyberataku czy oszustwa.

ⓘ Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni częściej niż kobiety udaliby się na do CSIRT i innych służb państwowych (32 vs 19%), dostawców usług internetowych jak operatorzy sieci komórkowych czy stacjonarnych (25 vs 17%) oraz do działu IT (18 vs 11%).

Panie częściej niż panowie skorzystałyby z pomocy rodziny lub krewnych (25 vs 16%) oraz znajomych posiadających wiedzę IT (23 vs 18%).

WIEK

Starsze osoby, w wieku ponad 60 lat, znacząco częściej niż najmłodsi Polacy, w wieku 18-29, skierowałyby się częściej na Policję lub inne lokalne organy ścigania (45 vs 38%), do instytucji finansowych lub banków (42 vs 28%) oraz dostawcy usług internetowych (30 vs 18%).

Osoby młodsze zdecydowanie częściej spróbowałyby rozwiązań problem samemu (29 vs 7%) lub skierowałyby się do działu IT (18 vs 7%). To również osoby młode częściej niż osoby starsze nie podjęłyby żadnych działań (9 vs 2%).

MIEJSCE ZAMIESZKANIA

Mieszkańcy największych miast (powyżej 500 tyś. mieszkańców) częściej niż mieszkańcy wsi skierowaliby się do CSIRT i innych służb państwowych (33 vs 24%), działu IT pracodawcy (21 vs 13%) czy dostawcy usług internetowych (25 vs 19%.

Z kolei mieszkańcy wsi częściej udaliby się na Policję lub do innych lokalnych organów ścigania (43 vs 33%) i trochę częściej nie podjęliby żadnych działań (5 vs 1%).

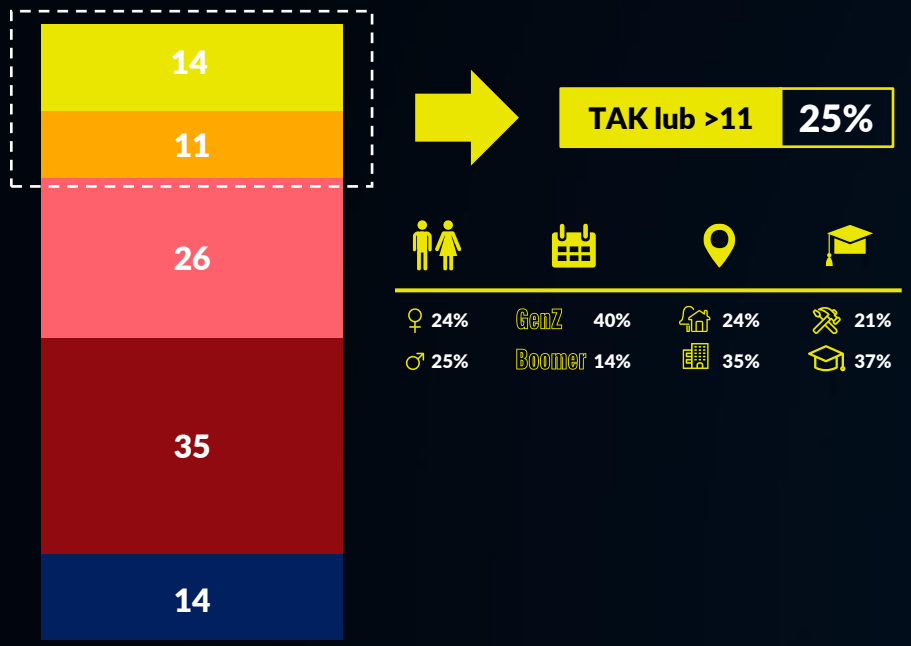
WYKSZTAŁCENIE

Największe różnice w zachowaniu można zaobserwować w podziale na rodzaj wykształcenia.

Polacy z wyższym wykształceniem znacząco częściej niż posiadający podstawowe wykształcenie udaliby się na Policję lub do innych lokalnych organów ścigania (46 vs 26%), znajomych z wiedzą IT (27 vs 11%), służb państwowych takich jak CSIRT (29 vs 17%) czy działu IT pracodawcy (22 vs 12%).

Z kolei osoby z wykształceniem podstawowym znacząco częściej skontaktowałyby się z dostawcą usług internetowych (35 vs 18%) czy profesjonalną firmą świadczącą usługi z zakresu cyberbezpieczeństwa (22 vs 8%).

Wiedza na temat posiadanych kont w internecie do komunikowania się, płacenia rachunków, nawiązywania kontaktów, zakupów online czy rezerwacji



Co czwarty Polak ma zbyt dużo kont lub więcej jak jedenaście. 14% Polaków nie kontroluje już liczby kont jakimi się posługuje co ułatwia cyberataki.

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Mateusz Zubkowicz

Client Business Partner, GfK

Ocena stanu wiedzy na temat bezpieczeństwa w internecie przyjmuje rozkład niemal normalny: 33% ocenia ją jako niską, a 28% twierdzi, że jest wysoka. Tylko 6% uważa się za ekspertów, co wskazuje na potrzebę dalszej edukacji w tej dziedzinie. Warto zauważyć, że mężczyźni częściej niż kobiety oceniają swoją wiedzę jako dużą lub ekspercką.

W przypadku testu z rozpoznania phishingu 55% osób nie jest pewna, czy e-mail, który przyszedł rzekomo od Netflixa, jest prawdziwy, a 24% od razu wskazała, że jest to scam. Aż 21% twierdzi, że ten mail jest poprawny i nie wzbudził ich wątpliwości. To pokazuje, że niestety tego typu ataki mogą mieć wysoką skuteczność i należy nadal prowadzić działania edukacyjne w tym obszarze. Optymistyczną informacją w tym kontekście jest to, że 66% Polaków jest chętnych do pogłębiania swojej wiedzy w zakresie cyberbezpieczeństwa.

W przypadku cyberataku 23% badanych twierdzi, że zna procedury postępowania, 20% ma osobę bliską lub znajomą, do której może zwrócić się o pomoc, a 18% wie, do jakich służb państwowych powinno się zgłosić. Z drugiej strony 22% w takiej sytuacji czułoby się zagubione, a 28% w ogóle nie wyobraża sobie takiej sytuacji. Pokazuje to, że nadal są potrzebne kampanie informacyjne mówiące o tym, gdzie szukać pomocy w przypadku cyberataku.

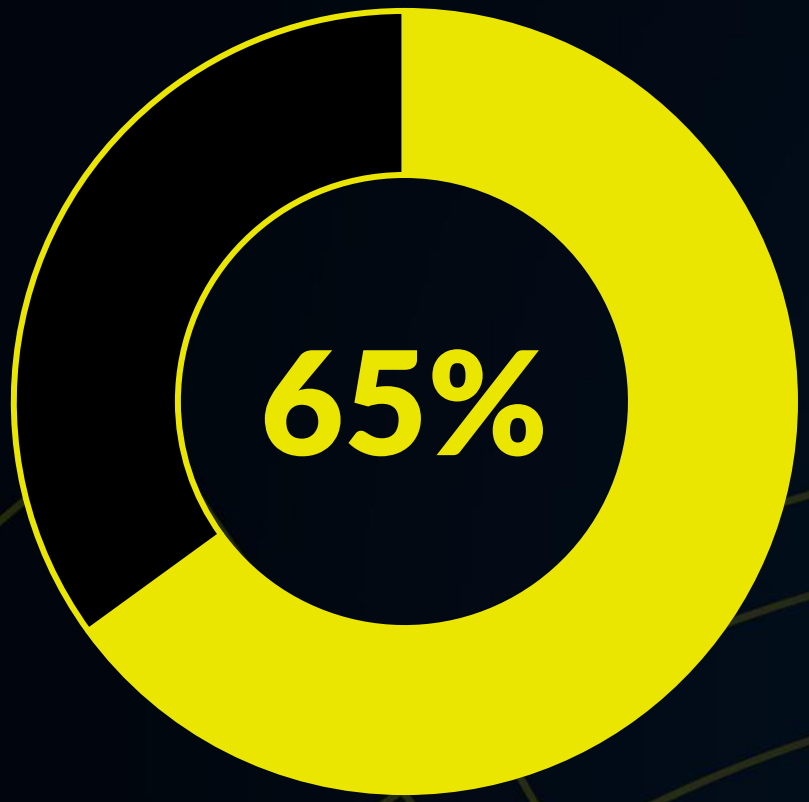
Optymistyczny jest wynik mówiący o tym, że w przypadku cyberataku 94% Polaków zgłosiłoby się gdzieś po pomoc. Najwięcej, bo 41% respondentów do lokalnych organów ścigania, a 38% do banku lub instytucji finansowej. Tylko 25% wie, do kogo zgłosić się w służbach państwowych, co sugeruje, że istnieje potrzeba lepszego informowania społeczeństwa o dostępnych zasobach i procedurach.

35% respondentów posiada tylko cztery lub mniej kont w internecie, a 26% ma od pięciu do dziesięciu kont. 14% uważa, że ma ich zdecydowanie zbyt dużo (22% spośród najmłodszej grupy w wieku 18–29 lat). Biorąc pod uwagę, że coraz więcej instytucji i usług wymaga od nas posiadania dedykowanego konta liczba ta będzie rosła, a więc będzie rosło też prawdopodobieństwo cyberataków.

Część dotyczącą wiedzy na temat bezpieczeństwa w Internecie można podsumować trzema słowami: edukacja, edukacja i jeszcze raz edukacja. Optymizmem napawa to, że Polacy są otwarci na zdobywanie nowej wiedzy w zakresie cyberbezpieczeństwa i jest to duża odpowiedzialność państwa, ale również firm i instytucji, aby szerzyć wiedzę o bezpieczeństwie w sieci i kształtować dobre nawyki.

2.2.

Czy czujemy się bezpiecznie w sieci i czy ma to wpływ na naszą aktywność?



Większość z nas martwi się o swoje bezpieczeństwo w internecie.

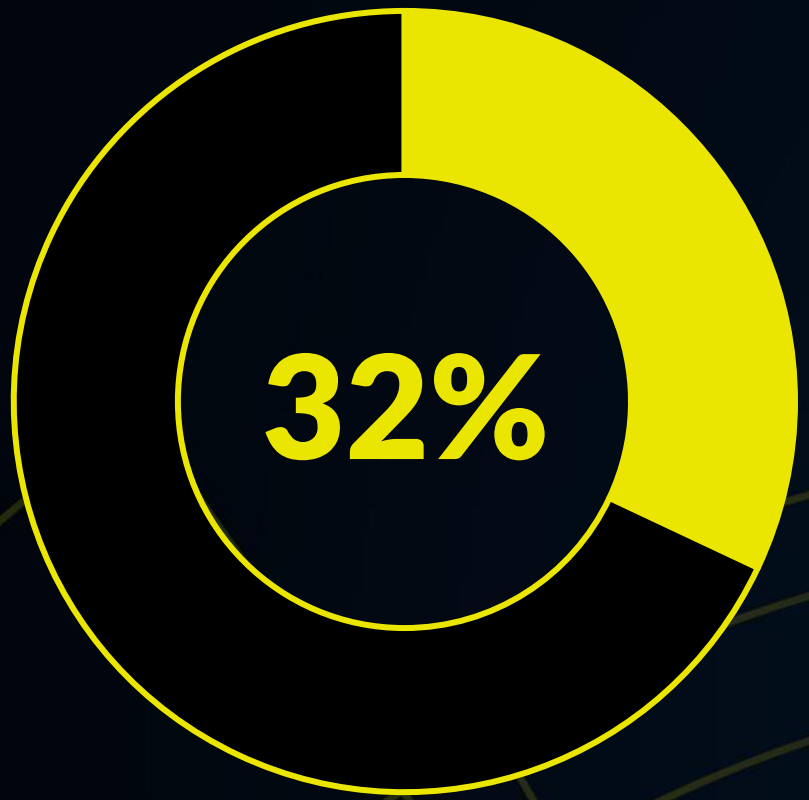
♀ 69%
♂ 61%

GenZ 55%
Boomer 76%

67%
61%

63%
63%

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)



Co trzeci Polak ograniczа swoją aktywność w związku z obawami o bezpieczeństwo w internecie.

♀ 33%
♂ 30%

GenZ 28%
Boomer 30%

30%
30%

35%
27%

Pytanie jednokrotnego wyboru
Baza: respondenci obawiający się o bezpieczeństwo (N=646).
Wartość następnie sprowadzona do N=1000.
49% ogranicza swoją aktywność spośród osób obawiających się o bezpieczeństwo.

Michał Kurek

Partner w Dziale Consultingu, szef Zespołu Cyberbezpieczeństwa w KPMG w Polsce i CEE

Obserwowany na całym świecie wzrost skali i złożoności cyberataków powoduje, że powszechne staje się poczucie zagrożenia podczas korzystania z usług cyfrowych. Niemal 2/3 Polaków niepokoi się o swoje bezpieczeństwo w internecie, przy czym co piąty obywatel odczuwa ten niepokój w stopniu poważnym. Hakerzy do przygotowania cyberataków wykorzystują zaawansowane techniki, takie jak sztuczna inteligencja czy informacje o lukach w bezpieczeństwie oprogramowania, na które nie ma jeszcze tzw. łat bezpieczeństwa. Dlatego ich skuteczność jest niezwykle wysoka. Z tej perspektywy niepokój użytkowników może cieszyć, prowadzi bowiem do zwiększonej ostrożności, która jest dziś niezbędna w cyfrowym świecie. Niestety, u ponad połowy zaniepokojonych użytkowników lęk ten prowadzi do ograniczenia aktywności w Internecie, a tym samym do utraty korzyści , jakie niosą nowoczesne usługi cyfrowe poprawiające komfort życia. W skali krajowej może to hamować dynamiczny rozwój cyfrowej gospodarki, zwłaszcza jeśli obawy te wynikają z braku wiedzy na temat cyberbezpieczeństwa. Przykładowo aż 38% Polaków postrzega korzystanie z usług bankowości elektronicznej za mało bezpieczne. Tymczasem przy dzisiejszych zabezpieczeniach stosowanych przez banki oraz zachowaniu podstawowej ostrożności trudno znaleźć bezpieczniejsze usługi cyfrowe.

Optymizmem napawa fakt, że źródła obaw Polaków związanych z korzystaniem z Internetu są uzasadnione. Nasi obywatele najbardziej obawiają się kradzieży tożsamości, infekcji złośliwym oprogramowaniem oraz wyłudzeń finansowych lub danych osobowych. Są to najczęściej występujące dziś cyberzagrożenia, co świadczy o dobrej intuicji lub adekwatnej wiedzy Polaków w tym zakresie. Zastanawia jednak relatywnie niski poziom obaw wobec dezinformacji, w tym tej wspartej zaawansowanymi technikami AI, tzw. deep fake. Zagrożenia te są dziś powszechne, a mogą prowadzić do napięć społecznych, podważenia wiarygodności mediów, a nawet do zagrożenia demokracji. Powinniśmy je więc traktować bardzo poważnie.

Jedynie co dwudziesty Polak nie ma żadnych obaw związanych z korzystaniem z usług cyfrowych. Prawdopodobnie grupa ta w niedługim czasie zmieni swoje nastawienie do cyberzagrożeń, zgodnie przysłowiem Polak mądry po szkodzie.

Kluczowego znaczenia nabiera więc właściwa edukacja społeczeństwa w zakresie cyberbezpieczeństwa, którą należy wprowadzać na jak najwcześniejszych etapach życia. Tak jak uczy się małe dzieci bezpiecznego przechodzenia przez jezdnię, tak samo powinno się wpajać podstawowe zasady cyberbezpieczeństwa. Rozwój technologii jest na tyle dynamiczny, że pozostawienie tych kwestii wyłącznie rodzicom będzie nieskuteczne, sami bowiem wymagają ciągłej edukacji w tym zakresie. Przy zachowaniu ostrożności opartej na wiedzy o możliwych cyberzagrożeniach i świadomym korzystaniu z dostępnych zabezpieczeń można relatywnie bezpiecznie korzystać z korzyści cyfryzacji

Czego najbardziej obawiają się Polacy korzystając z internetu?

TOP 3

Najbardziej obawiamy się o kradzież tożsamości lub przejęcie konta (61%), zainstalowania złośliwego oprogramowania (55%) lub wyłudzenia bądź kradzieży pieniędzy (54%).

Jedynie 4% Polaków deklaruje, że nie obawia się niczego.

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Kobiety częściej niż mężczyźni boją się o różnego rodzaju aktywności. Największe różnice na korzyść kobiet zaobserwowano dla obaw związanych z użyciem wizerunku do stworzenia deepfake (34 vs 22%), wyłudzeniem lub utratą swoich danych osobowych (50 vs 40%), kradzieży tożsamości lub przejęcia konta (65 vs 56%) oraz zainstalowania wirusa lub innego złośliwego oprogramowania (57 vs 52%).

WIEK

Osoby młodsze zdecydowanie częściej obawiały się mowy nienawiści, naruszenia własnej godności osobistej, ośmieszenia czy zastraszenia (32 vs 17%), ogólnie deepfake i fałszywych wiadomości (18 vs 11%) oraz dezinformacji (40 vs 35%).

Starsze osoby, w wieku ponad 60 lat, znacząco częściej niż najmłodsi Polacy, w wieku 18-29, obawiały się wyłudzenia lub utraty danych osobowych (53 vs 40%), wyłudzenia lub utraty kradzieży pieniędzy z banku, funduszu czy ubezpieczyciela (54 vs 45%) oraz zainstalowania wirusa lub innego złośliwego oprogramowania (58 vs 49%).

MIEJSCE ZAMIESZKANIA

Mieszkańcy największych miast (powyżej 500 tyś. mieszkańców) częściej niż mieszkańcy wsi obawiają się awarii usług i aplikacji w internecie kiedy będą ich potrzebować (30 vs 23%) oraz niekontrolowanego wycieku danych ze sklepu, serwisu, aplikacji (36 vs 32%).

Z kolei mieszkańcy wsi obawiają się użycia ich wizerunku do stworzenia deepfake z wykorzystaniem sztucznej inteligencji (33 vs 21%), mowy nienawiści, naruszenia ich godności osobistej, ośmieszenia, zastraszenia (23 vs 16%) i kradzieży pieniędzy z banku, funduszu lub ubezpieczyciela (59 vs 52%).

WYKSZTAŁCENIE

Polacy z wyższym wykształceniem znacząco częściej niż posiadający podstawowe wykształcenie boją się wyłudzenia i kradzieży pieniędzy z banku, funduszu lub ubezpieczyciela (59 vs 45%), niekontrolowanego wycieku danych ze sklepów, serwisów, aplikacji (35 vs 24%), zainstalowania wirusa lub innego złośliwego oprogramowania (61 vs 51%).

Z kolei osoby z wykształceniem podstawowym częściej obawiały się utraty prywatności (39 vs 34%) czy wyłudzenia lub utraty danych osobowych (56 vs 51%).

Renata Kania

Cybersecurity – Awareness Senior Specialist (Product Manager), T-Mobile Polska

Internet na przestrzeni lat stał się dla nas nie tylko narzędziem komunikacji i rozrywki, lecz także nieodłączną częścią pracy i codzienności wielu osób oraz działalności firm. W obliczu prezentowanych w raporcie statystyk i coraz większej roli technologii w życiu codziennym – niezależnie od wieku, płci czy miejsca zamieszkania – wręcz krytyczne stało się zagadnienie bezpieczeństwa w sieci. Rozwój technologiczny generuje tyle samo korzyści, co i zagrożeń, czego musimy mieć świadomość. Zadaniem każdej firmy technologicznej jest nie tylko dostarczanie innowacyjnych rozwiązań, lecz także kompleksowe dbanie o bezpieczeństwo użytkowników.

Jestem ekspertką do spraw świadomości zagrożeń i cyberbezpieczeństwa, której serce bije dla ludzi, bo doskonale wiem, jakie znaczenie ma każdy człowiek w całym łańcuchu bezpieczeństwa. Człowiek jest najważniejszym elementem całego systemu cyberbezpieczeństwa. Odnosząc się do deklaracji respondentów wskazujących, że 65% z nich ma obawy co do swojego bezpieczeństwa w internecie, a w konsekwencji tego 49% z nich ogranicza swoją aktywność w internecie, kreśli się gigantyczna przestrzeń do poprawy ich postrzegania bezpieczeństwa w sieci poprzez dostarczenie im narzędzi w postaci edukacji o świadomym, czujnym i umiejętnym postępowaniu wobec zagrożeń w świecie cyfrowym.

Naszą rolą jest dostarczać społeczeństwu najlepszej i niezawodnej sieci. A najlepszej to również – zabezpieczonej. Punktem wyjścia dla każdego użytkownika internetu powinna być znajomość i stosowanie zasad cyberhigieny. To podstawowe zadanie mogące uchronić przed główną obawą respondentów, z których 61% wskazują na kradzież tożsamości, która z kolei może spowodować negatywne skutki moralne i finansowe – aż 54% badanych obawia się utraty swoich pieniędzy. Badani wskazują jako mało bezpieczne te najpopularniejsze aktywności w internecie: korzystanie z bankowości elektronicznej (38%), zakupy online (36%), wiadomości online (30%) i korzystanie z mediów społecznościowych (27%).

Bezpieczeństwo zawsze zaczyna się od świadomości. Nie można być bezpiecznym, jeśli nie jest się świadomym. Poczucie bezpieczeństwa to poczucie świadomości. Reakcja w postaci zwątpienia czy nawet ograniczania aktywności w internecie powinna w każdym użytkowniku prowokować chęć i konieczność dodatkowej edukacji o właściwym i bezpiecznym korzystaniu z internetu, o sposobach radzenia sobie z zagrożeniem. Każdy z nas musi wypracować w sobie zdolność stanowienia swoim zasobom i swojej tożsamości indywidualnego Human Firewalla.

Aktywności w internecie postrzegane jako mało bezpieczne (1)

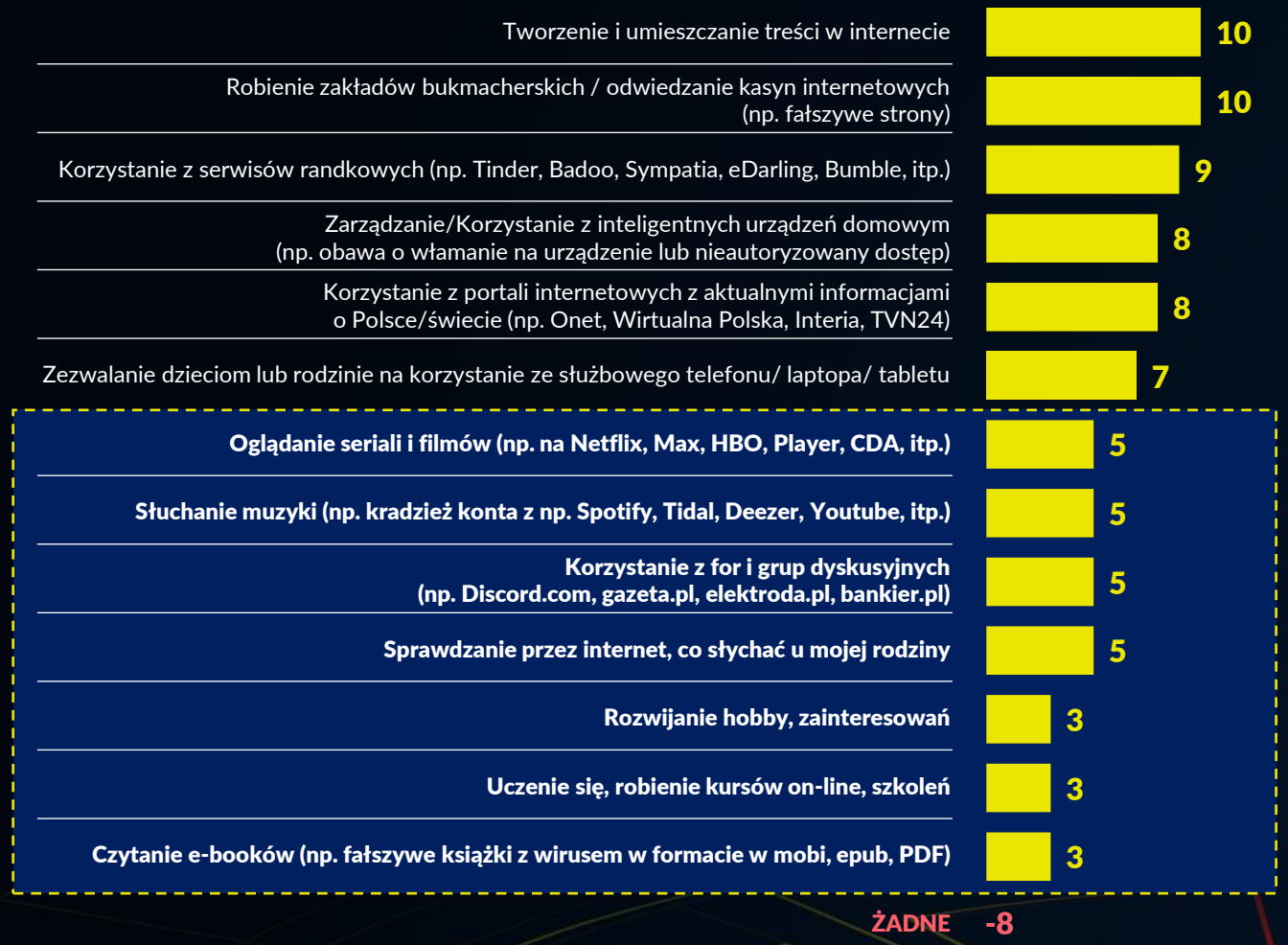
TOP 6

Najmniej bezpiecznie czujemy się podczas **korzystania z bankowości i płatności online (38%)** czy **robienia zakupów (36%).** **3 na 10 Polaków** obawia się korzystania z poczty elektronicznej. Około 1/4 Polaków jako mało bezpieczne aktywności uważa korzystanie z **mediów społecznościowych (27%), komunikatorów (23%) czy e-administracji.**

Jedynie 14% ma obawy podczas korzystania ze stron dla dorosłych.

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Aktywności w internecie postrzegane jako mało bezpieczne (2)



Najmniej obawiamy się o swoje bezpieczeństwo **korzystając z rozrywki** (filmy i seriale, muzyka, książki) czy rozwijając **swoje pasje (3%).**

Jedynie 7% obawia się zezwolenia dzieciom czy rodzinie **na korzystanie ze służbowego sprzętu.**

Również aktywność na serwisach **bukmacherskich** nie wzbudza u nas zbyt **dużych obaw (10%).**

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni częściej niż kobiety postrzegają za bardziej niebezpieczne takie aktywności jak korzystanie z serwisów randkowych (12 vs 7%) czy wysyłanie/odbieranie wiadomości e-mail (33 vs 27%).

Panie częściej niż panowie czują się mniej bezpiecznie przy korzystaniu z bankowości online (43 vs 32%), tzw. e-administracji (28 vs 19%) czy robieniu zakupów przez internet (39 vs 33%).

WIEK

Starsze osoby znacząco częściej niż najmłodsi Polacy czują się mniej bezpiecznie podczas korzystania z bankowości online (42 vs 29%), wysyłania/odbierania wiadomości e-mail (37 vs 25%), robienia zakupów online (39 vs 28%), e-administracji (28 vs 18%).

Osoby młodsze zdecydowanie częściej niż osoby starsze obawiały się o swoją aktywność podczas odwiedzania witryn i aplikacji zakładów bukmacherskich (18 vs 9%), wykonywania/odbierania połączeń głosowych lub SMS (15 vs 8%) czy tworzenia treści w internecie (17 vs 10%).

MIEJSCE ZAMIESZKANIA

Mieszkańcy wsi częściej niż mieszkańcy dużych miejscowości obawiają się o swoją aktywność w internecie podczas korzystania z bankowości online (42 vs 28%), robienia zakupów online (38 vs 31%), korzystania z mediów społecznościowych (30 vs 24%).

WYKSZTAŁCENIE

Największe różnice można zaobserwować z punktu widzenia wykształcenia.

Polacy z wyższym wykształceniem znacząco częściej niż posiadający wykształcenie podstawowe obawiają się o swoją aktywność w internecie podczas robienia zakupów (46 vs 21%), korzystania z bankowości online (43 vs 28%), korzystania z mediów społecznościowych (33 vs 23%) oraz grania w gry (12 vs 5%).

Tomasz Zieliński

Pilot paralotniowy, autor bloga Informatyk Zakładowy (informatykzakladowy.pl), programista z dwudziestoletnim stażem

Czym jest poczucie bezpieczeństwa? Paralotniarz szybujący kilometr nad pasmem górskim może czuć się bezpiecznie, tak samo wspinacz odpoczywający na skalnej półce na skraju przepaści. Obiektywnie rzecz biorąc, obaj podejmują spore ryzyko, więc ich osobiste bezpieczeństwo jest zagrożone.

W sportach ekstremalnych poczucie bezpieczeństwa idzie w parze z kontrolą nad otoczeniem. Pilot, wspinacz czy nurek ćwiczą umiejętności pod okiem instruktorów, potem samodzielnie powtarzają elementy szkolenia, by wyrobić odruchy, poznają cechy sprzętu i granice własnej odwagi. Dostrzegają potencjalne niebezpieczeństwa i aktywnie im zapobiegają. Zawczasu planują działania na wypadek zagrożenia.

Niestety, poczucie bezpieczeństwa nie towarzyszy wyłącznie profesjonalistom. Wiele wypadków samochodowych było bezpośrednim następstwem faktu, że poczucie bezpieczeństwa sprawców wynikało z braku doświadczenia i wyobraźni. Kierowca, który nigdy nie ćwiczył wyprowadzania auta z poślizgu, nie rozpozna zwiastunów utraty przyczepności. Planowanie kryzysowe z gatunku „będziemy się tym martwić później" jest skazane na porażkę – ale przekonają się o tym jedynie ci, których kryzys rzeczywiście dosięgnie.

Bezpieczeństwo w internecie

Gdy mówimy o poczuciu bezpieczeństwa w internecie, względnie łatwo sklasyfikować 65% respondentów deklarujących niepokój. Są to osoby mające świadomość zagrożeń – wśród których prawidłowo identyfikują ryzyko przejęcia cyfrowej tożsamości, utraty pieniędzy lub danych. Jednocześnie osoby te nie mają dostatecznych kompetencji, by samodzielnie oszacować ryzyko konkretnego działania w określonych okolicznościach – np. logowania do własnego banku na służbowym laptopie kolegi przez publiczne WiFi.

Tym osobom możemy i powinniśmy pomagać. Elementarz jest zawsze taki sam: uczymy obsługi menedżera haseł i objaśniamy, dlaczego w każdym serwisie trzeba mieć inne hasło. Tłumaczymy zasady uwierzytelniania dwuskładnikowego i kategorycznie zakazujemy przekazywania komukolwiek haseł jednorazowych z SMS-ów. Zachęcamy do używania kluczy Fido U2F, które dają odporność na ataki socjotechniczne.

Niebezpieczeństwo w internecie

Większy problem będzie z grupą 26% respondentów, których temat bezpieczeństwa w internecie nie martwi. Zostawmy zawodowców potrafiących rozpoznawać i rozbrajać zagrożenia – stanowią niewielki procent społeczeństwa. Co jednak powiedzieć osobom (raczej mężczyznom, raczej w średnim wieku, raczej z większych miast), którzy problemu nie dostrzegają lub go umniejszają?

Uniwersalnym argumentem może być troska o dobro bliskich. Złodziej przejmie ci Facebooka albo Whatsappa? W kwadrans wyłudzi pieniądze od twoich przyjaciół. Grasz w pirackie gry ściągane z sieci? Ransomware pozbawi cię cyfrowych zdjęć z całej dekady. Zainstalujesz na komórce dziwną aplikację wskazaną przez rzekomego konsultanta z banku? Oszczędności straci cała rodzina.

Co zaś robimy, gdy takie argumenty trafią na podatny grunt i pacjent zechce zadbać o swoje cyfrowe bezpieczeństwo? Cóż, elementarz jest zawsze taki sam…

Konrad Płachecki

Dyrektor Biura Architektury i Systemów Cyberbezpieczeństwa, Bank Gospodarstwa Krajowego

Większość badanych osób deklaruje poczucie bezpieczeństwa w internecie, mimo że ponad połowa przyznało doświadczenie scamu osobiście. Dalsze rozważania pokażą, czy to poczucie bezpieczeństwa wynika z wiedzy o zagrożeniach, czy tylko samego przeświadczenia. Zdecydowanie największe poczucie zagrożenia, niezależnie od wieku, osoby wskazują w przypadku metod ataków skupiających się bezpośrednio na nich i różnorodnych kanałach płatniczych. Szczególnie ciekawe jest wskazanie bankowości elektronicznej jako tej potencjalnie najbardziej niebezpiecznej. Może być to podyktowane niepełną wiedzą na temat bezpieczeństwa komunikacji wykorzystującej *certificate pinning* i ochronę przed atakami MITM, co jest obecnie szeroko wykorzystywane przez bankowe aplikacje mobilne. To już niestety dość specjalistyczna wiedza. Dzięki przypinaniu certyfikatów i innym środkom ochrony, jak biometria behawioralna, aplikacje mobilne stają się bezpieczniejsze niż przeglądarkowe. Dlatego też banki przenoszą do aplikacji mobilnych tak ważne usługi bezpieczeństwa, jak czynniki wieloskładnikowego uwierzytelniania wielu operacji, dokonywanych także w tradycyjnej bankowości elektronicznej czy płatnościach kartami kredytowymi w internecie. Na komentarz zasługuje także fakt niskiego sklasyfikowania zagrożeń podszywania się pod numery telefoniczne. Wykorzystywana jest podatność protokołu komunikacyjnego w sieciach telefonicznych SS7, którą obecnie trudno zmitygować. Ataków wykorzystujących metodę „na konsultanta z banku" jest coraz więcej. Niektóre banki wykorzystują wspomniane aplikacje mobilne do weryfikowania dzwoniącego konsultanta, inne wprost ogłaszają, że ich konsultanci nigdy nie dzwonią. Poza tymi metodami pozostaje jedynie czujność potencjalnej ofiary na nietypowe zachowanie osoby dzwoniącej.

Podsumowując, warto zwrócić uwagę, że niezmiennie bardzo ważna jest stała edukacja w obszarze cyberbezpieczeństwa dopasowana dla osób w różnych przedziałach wiekowych. Przede wszystkim pokazanie, że istnienie w cyberświecie to ciągła analiza faktów, tego, co się może stać po moim działaniu, jak również to, czy mam wystarczającą wiedzę, czy coś się zmieniło od ostatniego razu – ciągła analiza i szacowanie ryzyka. To dalej uświadamianie na temat aktualnych zagrożeń, które ciągle ewoluują i będą ewoluować w przyszłości, aby wzbogacać wiedzę. O metodach minimalizowania ryzyka, aby łatwiej było je szacować i podejmować decyzje.

Opinie na temat cyberbezpieczeństwa

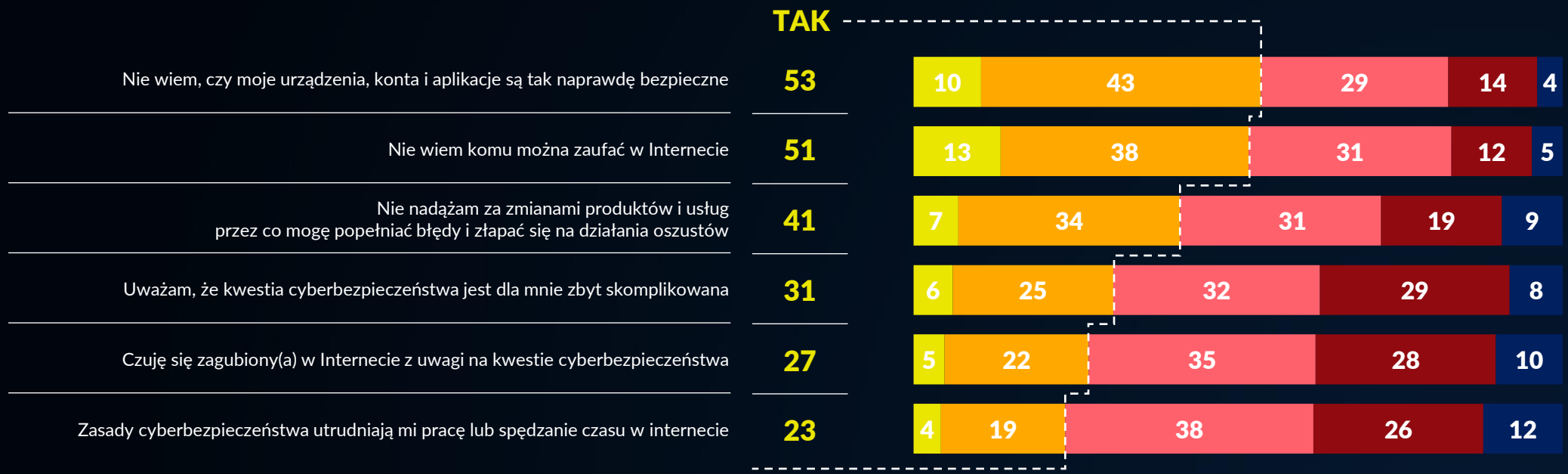
Ponad połowa Polaków nie wie komu ufać w sieci, ani czy ich urządzenia, konta i aplikacje są tak naprawdę bezpieczne.

4 na 10 Polaków nie nadąża za zmianami w cyfryzacji stąd popełnia błędy i jest **podatna na działania oszustów.**

3 na 10 Polaków jest zagubionych bo kwestie cyberbezpieczeństwa są **zbyt skomplikowane.**

Blisko **1 na 3 Polaków** stwierdza, że **zasady cyberbezpieczeństwa utrudniają im pracę** lub aktywność w sieci.

Opinie na temat cyberbezpieczeństwa



W wyniku zaokrągleń wskazania przy niektórych stwierdzeniach sumują się do 99%

Całkowicie się zgadzam
Raczej się zgadzam
Ani się zgadzam, ani się nie zgadzam
Raczej się nie zgadzam
W ogóle się nie zgadzam

Pytanie jednokrotnego wyboru na każde stwierdzenie.
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Kobiety zdecydowanie częściej niż mężczyźni odpowiedziały twierdząco na wszystkie przedstawione opinie w badaniu.

Największe zmiany na korzyść kobiet można zaobserwować dla opinii:

- „Nie wiem, czy moje urządzenia, konta i aplikacje są tak naprawdę bezpieczne" (61 vs 46%),
- „Nie wiem komu można zaufać w Internecie" (59 vs 44%),
- „Nie nadążam za zmianami produktów i usług przez co mogę popełniać błędy i złapać się na działania oszustów" (47 vs 35%)
- oraz „Czuję się zagubiony(a) w Internecie z uwagi na kwestie cyberbezpieczeństwa" (33 vs 21%).

WIEK

Osoby starsze częściej odpowiadały twierdząco niż osoby młodsze na przedstawione pytania.

Największe zmiany na korzyść osób starszych można zaobserwować dla opinii:

- „Uważam, że kwestia cyberbezpieczeństwa jest dla mnie zbyt skomplikowana" (47 vs 17%),
- „Nie nadążam za zmianami produktów i usług przez co mogę popełniać błędy i złapać się na działania oszustów" (55 vs 28%),
- „Nie wiem komu można zaufać w Internecie" (64 vs 45%),
- „Czuję się zagubiony(a) w Internecie z uwagi na kwestie cyberbezpieczeństwa" (35 vs 21%).

MIEJSCE ZAMIESZKANIA

Nie zaobserwowano większych różnic wśród respondentów z uwagi na miejsce zamieszkania. Jedyna znacząca różnica wystąpiła w opinii na temat czucia się zagubionym w internecie i wyniosła 11 punktów procentowych na korzyść osób mieszkających na wsi (31 vs 20%).

WYKSZTAŁCENIE

Największe różnice z uwagi na poziom wykształcenia można zaobserwować w przypadku opinii na temat zbyt dużego poziomu skomplikowania kwestii cyberbezpieczeństwa. Z tą opinią częściej zgadzały się osoby z podstawowym wykształceniem (36 vs 24%). Podobnie było w przypadku czucia się zagubionym (33 vs 24%) oraz braku zaufania w internecie (62 vs 53%).

dr Łukasz Olejnik, LL.M.

Niezależny badacz i konsultant, prowadzi bloga prywatnik.pl, związany z Department of War Studies King's College London, autor książek *Filozofia Cyberbezpieczeństwa* (PWN, 2022) i *Propaganda* (PWN, 2024)

Z badania wynika, że 51% badanych nie wie, komu można ufać w internecie, co idealnie pokrywa się z tym, co podkreśliłem w książce Filozofia Cyberbezpieczeństwa: ostrożność w stosunku do tego, co czytamy na ekranie w świecie cyfrowym, jest dobrą strategią obronną, szczególnie w erze wszechobecnych oszustw. Problem polega jednak na tym, że takie podejście grozi dalszą erozją zaufania w społeczeństwie lub, w przypadku Polski, negatywnie wpłynie na jego ewentualną poprawę.

Najwięcej problemów z zaufaniem wskazała grupa wiekowa 60–75 lat (64%), co jest zrozumiałe, ponieważ to oni często mogą stać się celem cyberprzestępców. Jak można mieć zaufanie, nie wiedząc do końca, jak działają technologie i IT?

Właśnie to sygnalizuje inny element badania: 41% badanych przyznaje, że nie nadąża za szybkimi zmianami w produktach i usługach. Może to prowadzić do pomyłek, które mogą mieć opłakane skutki dla prywatnych danych lub finansów. Jest to ważny sygnał dla firm. Te powinny wprowadzać nowe technologie w sposób ostrożny i odpowiedzialny, bez radykalnych przeprojektowań, np. nagłych zmian w interfejsie użytkownika, które mogą dezorientować użytkowników. Respondenci często wskazują, że wolą korzystać z rozwiązań, które dobrze znają, zamiast uczyć się nowych. I to ma sens. Chcą korzystać z technologii, a nie tracić życie na dostosowywanie się do zmian, które wymyślił sobie zespół projektowy. Mało co denerwuje bardziej niż zakłócanie już wypracowanego sposobu korzystania z urządzeń i oprogramowania.

dr Agnieszka Jankowska

Członkini zarządu fundacji Digital Poland ds. edukacji cyfrowej, dyrektorka ds. korporacyjnych i public affairs, T-Mobile Polska, przewodnicząca Rady ds. Cyfryzacji przy Ministerstwie Cyfryzacji

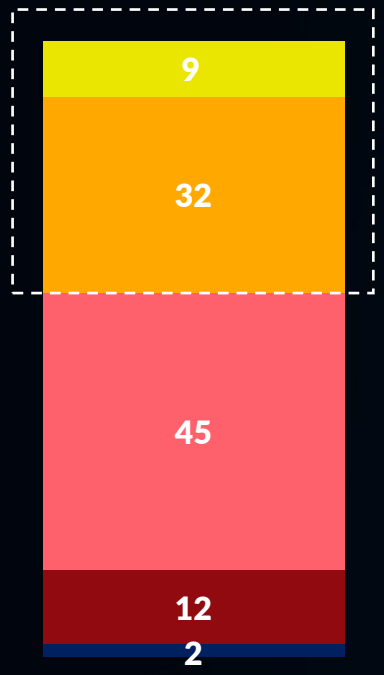
Ponad połowa Polaków (53%) nie jest pewnych, czy ich urządzenia i konta są bezpieczne, a 51% nie wie, komu zaufać w sieci. To niepokojący wynik, który znajduje odzwierciedlenie również w badaniach realizowanych w skali Unii Europejskiej. Z raportu „Cybersecurity Barometer 2023", opublikowanego przez Eurostat, wynika, że średnio 54% obywateli UE ma wątpliwości co do bezpieczeństwa swoich urządzeń i kont. Jest to wyraźna informacja dla instytucji publicznych oraz dla przedsiębiorstw, że powinni lepiej komunikować użytkownikom, w jaki sposób mogą zabezpieczyć swoje dane oraz jak można weryfikować wiarygodność podmiotów funkcjonujących w cyberprzestrzeni. Działania edukacyjne w tym zakresie są niezbędne, ponieważ brak wiedzy lub niewystarczająca wiedza na temat potencjalnych cyberzagrożeń oraz sposobów chronienia się przed nimi, może sprzyjać ryzykownym zachowaniom, takim jak korzystanie z niesprawdzonych, niezabezpieczonych stron internetowych, ignorowanie ostrzeżeń lub zbyt pochopne udostępnianie swoich danych.

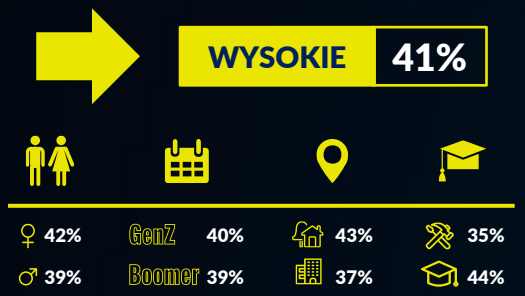
Działania na rzecz edukowania społeczeństwa są tym bardziej istotne, że z niniejszych badań wynika, że blisko 27% Polaków czuje się zagubionych w kwestiach związanych z cyberbezpieczeństwem. Jednocześnie, jak wynika z raportu Komisji Europejskiej, unijne przepisy dotyczące ochrony danych osobowych (RODO) przyczyniły się do zwiększenia przejrzystości w zakresie korzystania z tych danych, aczkolwiek zrozumienie tych przepisów nadal jest problematyczne dla wielu obywateli. Dla części użytkowników zasady te mogą wydawać się skomplikowane i trudne do zrozumienia, co potwierdza również niniejsze badanie, w którym co czwarta osoba uważa, że cyberbezpieczeństwo utrudnia jej korzystanie z internetu.

2.3.

Jak jesteśmy atakowani i oszukiwani w internecie?

Ryzyko stania się ofiarą cyberataków, oszustw, cyberprzestępczości czy kradzieży danych





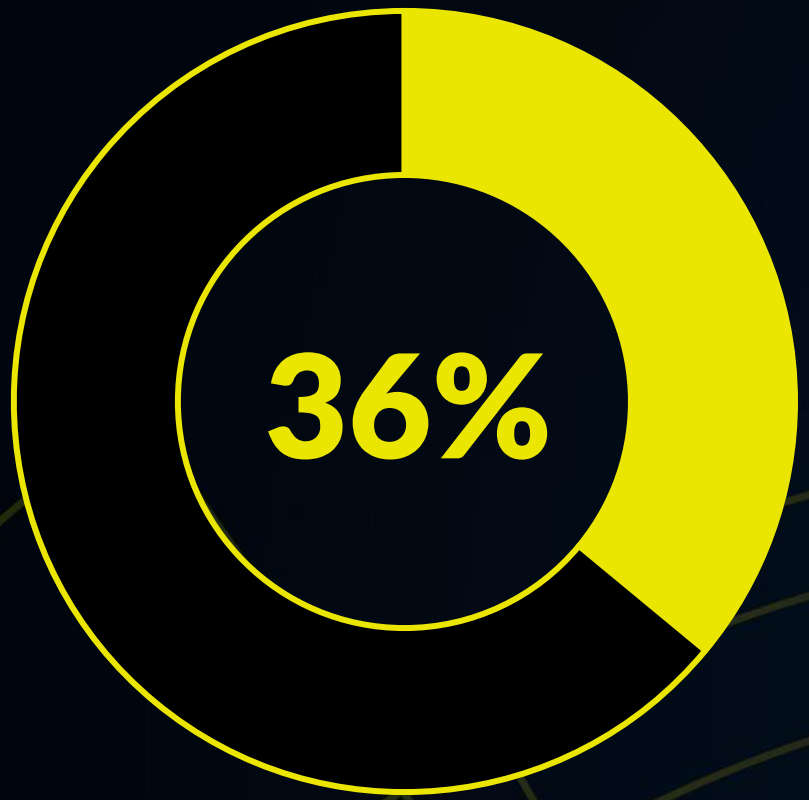
Jedynie 14% Polaków czuje się niezagrożonych atakami.

4 na 10 Polaków ocenia zmaterializowanie się takiego ryzyka za wysoce prawdopodobne.

Bardzo wysokie
Niskie
Umiarkowane
Niskie
Bardzo niskie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Czy doświadczono cyberataków, oszustw w sieci, incydentów w ciągu ostatnich 12 miesięcy?



DEFINICJA CYBERATAKÓW LUB INCYDENTÓW DLA RESPONDENTA*

- Odnoszą się do wszelkich nieautoryzowanych lub złośliwych działań, które zagrażają bezpieczeństwu, prywatności lub funkcjonalności urządzeń cyfrowych, kont internetowych lub danych osobowych.
- Incydenty te mogą skutkować kradzieżą danych, stratami finansowymi, naruszeniem prywatności lub zakłóceniem normalnej aktywności online. Można do nich zaliczyć: otrzymywanie fałszywych e-maili, wiadomości (phishing), wirusy lub oprogramowanie ransomware, które może zainfekować urządzenie i spowodować szkody, wyciek danych osobowych, haseł, kradzież tożsamości internetowej i przejęcie kont, wszelkie oszustwa internetowe próbują nakłonić użytkownika do przekazania pieniędzy lub danych osobowych.

* pytanie zadano po podaniu definicji

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Rodzaje doświadczonych cyberataków, oszustw w sieci, incydentów w ciągu ostatnich 12 miesięcy

TOP 3

Najczęstszą formą ataku był phishing (41%), scam (38%) oraz spoofing (27%). W co piątym przypadku było to przejecie konta (np. w mediach społecznościowych, e-sklepie, forum itp.).

Pytanie wielokrotnego wyboru
Baza: doświadczyli ataku (N=359)

PŁEĆ

Największe różnice w podziale na płeć zaobserwowano na korzyść panów dla ataku w postaci scamu (49 vs 23%), szantażu (20 vs 10%) oraz wycieku danych (14 vs 6%).

Panie częściej niż panowie wskazały, że zainstalowano u nich na urządzeniu elektronicznym złośliwe oprogramowanie (13 vs 6%).

WIEK

Starsze osoby częściej niż osoby młodsze wskazały, że zainstalowano na ich urządzeniu wirusa (17 vs 7%), szantażowano ich (22 vs 16%) czy doświadczono manipulacji lub inżynierii społecznej (17 vs 12%).

Osoby młodsze zdecydowanie częściej od osób starszych wskazały, że spotkały się z phishingiem (47 vs 28%), przejęto ich konta (24 vs 8%) czy zaobserwowano atak DDoS (23 vs 9%). Podobnie częściej zaobserwowano zjawisko spoofing (33 vs 20%).

MIEJSCE ZAMIESZKANIA

Osoby z dużych miejscowości częściej wskazały, że stały się obiektem ataków w ciągu ostatnich dwunastu miesięcy. Największe różnice na korzyść osób z dużych miast można zaobserwować w przypadku scamu (56 vs 39%), phishingu (56 vs 44%) czy szantażu (21 vs 13%).

Osoby mieszkające na wsi częściej wskazały, że przejęto ich konta w mediach społecznościowych lub w internecie (19 vs 3%), zaobserwowano spoofing (31 vs 19%) czy doświadczono manipulacji lub inżynierii społecznej (13 vs 4%).

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem częściej niż osoby z podstawowym wykształceniem wskazały, że doświadczyły phishingu (55 vs 26%), spoofingu (31 vs 12%) czy wyciekły ich dane osobowe (12 vs 3%).

Osoby z wykształceniem podstawowym częściej wskazały, że doświadczyły scamu (49 vs 31%), kradzieży tożsamości (18 vs 2%) czy złośliwego oprogramowania (23 vs 9%).

Adam Haertle

Ekspert bezpieczeństwa z ponad dwudziestoletnim doświadczeniem, prelegent, trener i wykładowca, twórca i redaktor naczelny serwisu ZaufanaTrzeciaStrona.pl. Organizuje jedną z największych polskich konferencji poświęconych bezpieczeństwu – Oh My H@ck (omhconf.pl)

Ryzyko stania się ofiarą ataków i oszustw w internecie wysoko lub bardzo wysoko ocenia tylko 41% respondentów. To dość optymistyczne podejście – najwyraźniej Polki i Polacy mają dużą wiarę w swoje umiejętności zachowania bezpieczeństwa w sieci. Z drugiej strony podobna liczba, bo 36% respondentów, potwierdza, że w ostatnim roku bezpośrednio doświadczyło oszustw lub innych ataków w internecie. To ciekawy wynik – wiemy, że z sieci w Polsce korzysta znacznie większy odsetek obywateli, więc można się zastanawiać, kim są ci, którzy ataków nie doświadczyli. Praktycznie każda skrzynka e-mailowa i większość numerów telefonów są bombardowane szerokim spektrum złośliwych wiadomości. Czy zatem 64% Polek i Polaków nie zauważa prób ataków? To nie byłby dobry wynik.

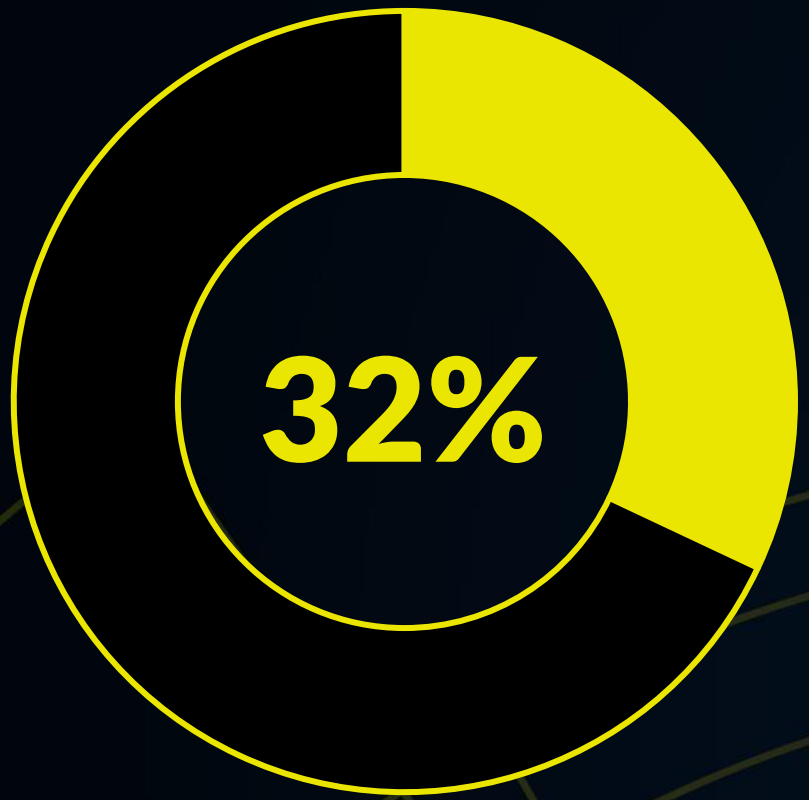
Badane osoby jako najczęściej doświadczeni rodzaje ataków wskazują wiadomości SMS i e-mail, fałszywe reklamy oraz połączenia telefoniczne – to zestaw odpowiedzi, którego należy się spodziewać. Niepokojące jest jednak to, że aż 20% respondentów doświadczyło przejęcia konta w serwisie online – to pokazuje ogromną skalę tego rodzaju ataków i niski poziom zabezpieczeń naszych danych w sieci. Podobnie niepokojące jest to, że 32% ankietowanych otrzymało już informację o kradzieży lub wycieku swoich danych osobowych.

Zawdzięczamy to oczywiście RODO, zmuszającemu usługodawców do przekazywania ofiarom takiej informacji. Można się spodziewać, że liczba ta będzie istotnie rosnąć w kolejnych latach.

Co ciekawe, na pytanie, czy doświadczyli osobiście scamu w sieci, aż 56% respondentów potwierdziło. Stoi to w kontraście do 36%, które doświadczyło oszustw lub innych ataków i pokazuje, że im dokładniej pytamy, tym więcej osób przypomina sobie, że jednak coś złego je w internecie spotkało. Trudno dzisiaj korzystać z internetu bez napotykania się na każdym kroku na próby oszustwa, nie dziwi zatem taka skala pozytywnych odpowiedzi. Najczęściej wskazywanymi kanałami otrzymania scamu były fałszywe e-maile, SMS-y i wiadomości w komunikatorach. Z kolei wśród rodzajów scamu respondenci wskazywali przede wszystkim fałszywe konkursy, phishingi oraz oszustwa związane z zakupami. To ciekawy ranking, ponieważ odpowiedź z góry listy, czyli fałszywe konkursy, nie wydaje się być zbyt oczywista i rzadko stanowi przedmiot działań organów ścigania.

Zdecydowana większość odbiorców nie tylko zauważa, że skala scamu od lat nieprzerwanie rośnie, lecz także prognozuje pogarszanie się tej sytuacji. Za główny powód tego zjawiska uważają oni nieostrożność użytkowników i brak zabezpieczeń systemów i urządzeń. Co ciekawe, wśród powodów nie pojawia się np. niska wykrywalność sprawców tych przestępstw lub bezkarność dużych platform internetowych, które nie tylko wolno ścigają oszustów, lecz także czerpią korzyści z ich działania, np. sprzedając im usługi reklamowe. Aż 73% respondentów uważa, że dostawcy usług tacy jak Google, Facebook, X czy TikTok powinni zostać poddani regulacjom i karom, skłaniającym ich do skuteczniejszego i szybszego reagowania na oszustwa na ich platformach.

Czy kiedykolwiek poinformowano Polaków o kradzieży lub też wycieku danych osobowych?



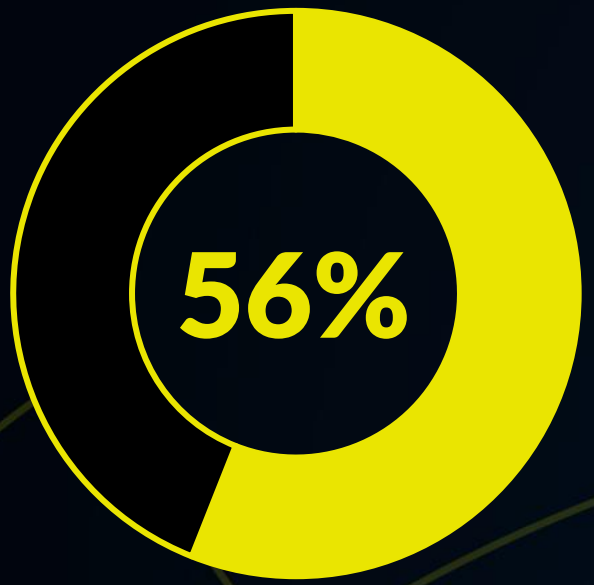
DEFINICJA WYCIEKU DANYCH DLA RESPONDENTA*

- **Jest to nieautoryzowane ujawnienie, dostęp lub utrata danych osobowych lub poufnych.** Może to obejmować kradzież informacji przez hakerów, np. wyciek danych klientów ze sklepu internetowego, przypadkowe ujawnienie przez pracowników lub inne formy naruszenia zabezpieczeń.
- **W efekcie osoby nieuprawnione mogą uzyskać dostęp do informacji, co może prowadzić do ich niezgodnego z prawem wykorzystania.** Wyciek danych często wiąże się z ryzykiem utraty prywatności, strat finansowych i naruszeniem reputacji.

* pytanie zadano po podaniu definicji

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Czy kiedykolwiek osobiście doświadczono scamu?



♀ 53%
♂ 59%

GenZ 68%
Boomer 43%

57%
57%

45%
66%

DEFINICJA SCAMU DLA RESPONDENTA*

Scam to każda forma oszustwa, która ma na celu wyłudzenie pieniędzy, danych osobowych lub odniesienia innych korzyści od ofiary oszusta. Scam dokonuje się najczęściej przez internet czy telefon. Oszustwa przybierają różne formy i są realizowane poprzez różne techniki manipulacyjne.

Do scamów można zaliczyć np.

- **phishing**, który polega na podszywaniu się pod osobę, firmę lub instytucję np. w e-mailu w celu wyłudzenia danych osobowych, haseł, kart kredytowych,
- **fałszywe reklamy**, które promują fałszywe lub nieprawdziwe produkty, wykorzystują wizerunek znanej osoby, zachwalają szybkie zyski z inwestycji,
- **oszustwa związane z pracą** (również tymczasową), które np. reklamują wysokie zarobki za niewielką pracę, a np. wymagają opłaty rejestracyjnej,
- **fałszywe konkursy, promocje**, które oferują np. nieprawdziwe zniżki lub nagrody, których celem jest wyłudzenie danych do płatności
- **fałszywe sklepy internetowe**, które udają prawdziwe sklepy internetowe, ale po dokonaniu zakupu klient nie otrzymuje towaru lub otrzymuje podróbki
- **oszustwa randkowe**, w których jedna z osób podaje się za kogoś innego celem zmanipulowania drugiej osoby i wyłudzenia pieniędzy,
- **fałszywe wsparcie techniczne**, które powiadamia użytkownika o niby zawieszeniu jego konta w serwisie społecznościowym lub innym celem wyłudzenia jego danych,
- **oszustwa telefoniczne**, w których osoba dzwoniąca podaję się za kogoś innego np. przedstawiciela banku, celem wyłudzenia danych do logowania ofiary.

* pytanie zadano po podaniu definicji

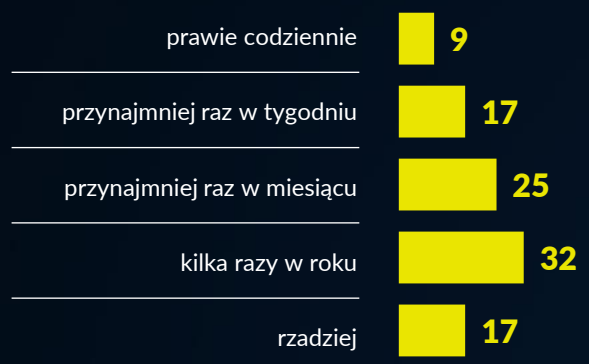
ⓘ Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Scam – gdzie i jak często?

Gdzie doświadczono na scamu?

ⓘ Pytanie wielokrotnego wyboru
Baza: doświadczyli scamu (N=559)

Jak często natrafiono na scam?



ⓘ Pytanie jednokrotnego wyboru
Baza: doświadczyli scamu (N=559)

Połowa doświadczyła scamu **poprzez e-mail,** a blisko **co trzeci** przez **SMS lub komunikator.**

Co czwarty scam to **fałszywa reklama** czy zakup.
Jedynie 17% doświadczyło scamu rzadziej niż **kilka razy w roku.**

PŁEĆ

Mężczyźni częściej niż kobiety atakowani byli poprzez fałszywą wiadomość e-mail (57 vs 41%), napotkali fałszywe reklamy w internecie (30 vs 16%) oraz fałszywe strony www (27 vs 14%). Kobiet trochę częściej doświadczyły fałszywej rozmowy telefonicznej (29 vs 25%).

Z punktu widzenia częstotliwości natrafienia na scam to mężczyźni wskazywali, że częściej go obserwują gdyż przynajmniej raz w miesiącu (58 vs 44%).

WIEK

Osoby starsze częściej doświadczyły scamu w postacie fałszywej wiadomości e-mail (57 vs 39%) czy fałszywej rozmowy telefonicznej (31 vs 21%).

Osoby młodsze częściej doświadczyły scamu w postaci fałszywej wiadomości w komunikatorze internetowym (36 vs 19%), fałszywego zakupu na platformie zakupowej (26 vs 9%) czy fałszywej strony www lub reklamy w internecie – w obu przypadkach różnica wyniosła dziewięć punktów procentowych.

Osoby młodsze częściej niż osoby starsze doświadczyły scamu przynajmniej raz w miesiącu (55 vs 47%).

MIEJSCE ZAMIESZKANIA

Osoby z dużych miejscowości częściej doświadczyły scamu w postaci fałszywych zakupów na platformie zakupowej (33 vs 23%), fałszywej wiadomości SMS/MMS (46 vs 38%) czy fałszywej wiadomości w komunikatorze internetowym (24 vs 20%).

Osoby zamieszkujące wsie częściej niż osoby zamieszkujące duże miasta doświadczyły scamu przynajmniej raz w miesiącu (52 vs 43%).

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem zdecydowanie częściej doświadczyły scamu w postaci fałszywej rozmowy telefonicznej (34 vs 11%), fałszywej wiadomości SMS/MMS (47 vs 25%).

Osoby z wykształceniem podstawowym częściej doświadczyły scamu poprzez fałszywą wiadomość e-mail (57 vs 46%) czy fałszywy wpis na mediach społecznościowych (22 vs 13%).

Osoby z wyższym wykształceniem częściej doświadczyły scamu przynajmniej raz w miesiącu (52 vs 40%).

dr inż. Jerzy Żurek

Ekspert ICT, doradca zarządów Asseco Poland i Netia

Badanie przeprowadzone dla fundacji Digital Poland dotyczy wielu aspektów szeroko rozumianego cyberbezpieczeństwa. Bardzo ciekawe i wartościowe informacje zawierają dane zaprezentowane w rozdziale Cyberataki i scam. Scam – to angielskie słówko w slangu fachowców od cyberbezpieczeństwa oznacza po prostu szeroko rozumiane oszustwa, które mają miejsce w sieciach teleinformatycznych, stałych i ruchomych w obszarach różnych usług stricte telekomunikacyjnych, jak również w szeroko rozumianym internecie.

Istotą scamu jest oddziaływanie na człowieka, takie, aby choć na chwilę zdobyć jego zaufanie lub wytworzyć presję, by podjął on decyzję o przekazaniu danych środków finansowych, rzeczy materialnych osobom do tego zupełnie nieuprawnionym. Wykorzystywane są w tym celu wszelakie kanały komunikacyjne funkcjonujące w cyberświecie, ale charakter oddziaływania ma naturę socjotechniczną. Osoba, która jest scamowana musi, chociaż na chwilę uwierzyć w przekazywane jej treści.

Należy zauważyć, że w tym przypadku nie jest wymagana żadna zaawansowana wiedza techniczna, która w przypadku cyberbezpieczeństwa kojarzy się z mitycznymi hakerami, którzy korzystają z zaawansowanych narzędzi informatycznych, przełamują kolejne złożone zabezpieczenia, łamią systemy kryptograficzne czy generują złożone klucze. Nie trzeba pisać zaawansowanego złośliwego oprogramowania czy przejmować tysięcy komputerów na całym świecie, żeby w odpowiednim momencie wykorzystać je do zmasowanego ataku na jakiś system. Nic z tych rzeczy – to po prostu czysta socjotechnika.

Mnogość typów takich ataków jest wielka, mimo że, jak wspomnieliśmy powyżej, są one rodzajowo ograniczone. Może to być telefon od osoby podszywającej się pod doradcę z banku (doświadczyli tego członkowie mojej rodziny) czy wyrafinowany e-mail do głównej księgowej w twojej organizacji, wysłany z „twojego" adresu, z poleceniem przelewu, dużej acz nie za dużej sumy pieniędzy, do firmy, z którą właśnie realizujecie projekt i rzeczywiście regularnie płacicie jej za realizowane zadania, które oczywiście są poprawnie opisane w fałszywym mailu (osobiście tego doświadczyłem).

Przeprowadzone badanie pokazuje, że właśnie ten rodzaj incydentów jest obecnie w różnego rodzaju sieciach najpowszechniejszy. Być może nie przynosi tak dużych strat finansowych jak ataki ransomware, ale z całą pewnością dotyczy i dotyka największej liczby użytkowników i zapewne w codziennym życiu jest społecznie najbardziej uciążliwy. Ciekawostką wynikającą z badania jest to, że najczęściej incydenty tego rodzaju identyfikują osoby z wyższym i średnim wykształceniem w średnich i małych ośrodkach miejskich.

Ważne jest, aby z tego cennego badania wyciągnąć właściwe wnioski i podjąć odpowiednie działania. Co możemy realnie zrobić, żeby przeciwdziałać scamowi? Na pewno powinniśmy edukować cyfrowo, intensywniej i z silniejszym podkreśleniem tej problematyki niż teraz. Zapewne powinniśmy pracować nad nowymi narzędziami (w tym AI) skuteczniej wykrywającymi scam i filtrującymi scamerskie wiadomości. Być może wyspecjalizowane zespoły w CSiRT-ach, wykrywające kampanie scamerskie, powinny o tym częściej i powszechniej informować. Z całą pewnością natomiast powinniśmy krytycznie myśleć o otrzymywanych wiadomościach, kierować się zdrowym rozsądkiem, a w sytuacjach wątpliwych weryfikować otrzymywane treści.

Jakiego rodzaju scamu doświadczono?

TOP 3

Co trzeci scam to fałszywy konkurs lub loteria, oszustwo phishingowe lub zakupowe.

Do popularnych form scamu można też zaliczyć oszustwo dodatkowego zarobkowania, inwestycyjne czy dotyczące płatności lub subskrypcji.

16% scamów to fałszywe akcje dobroczynne.

Pytanie wielokrotnego wyboru
Baza: doświadczyli scamu (N=559)

PŁEĆ

Mężczyźni częściej niż kobiety doświadczyli fałszywego konkursu lub loterii (46 vs 35%), oszustw inwestycyjnych (25 vs 14%) czy oszustw związanych z subskrypcją (21 vs 13%).

Kobiet częściej niż mężczyźni doświadczyły fałszywej akcji dobroczynnej (20 vs 13%) czy oszustwa na członka rodziny (16 vs 9%)

WIEK

Osoby starsze częściej niż osoby młode doświadczyły scamu w postaci fałszywej faktury czy dokumentu (23 vs 8%), fałszywej akcji dobroczynnej (28 vs 14%) czy fałszywego konkursu (57 vs 44%).

Osoby młodsze częściej niż osoby starsze spotkały się z oszustwem na członka rodziny czy przyjaciela (19 vs 8%) czy oszustwa związanego z pomocą techniczną (17 vs 10%).

MIEJSCE ZAMIESZKANIA

Osoby mieszkające w dużych miasta częściej doświadczyły fałszywego konkursu lub loterii (49 vs 36%), fałszywej akcji dobroczynnej (21 vs 13%) czy oszustwa inwestycyjnego (26 vs 18%).

Osoby mieszkające na wsi częściej doświadczyły oszustwa związanego z dodatkowym zarobkowaniem lub zatrudnieniem (31vs 22%).

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem częściej doświadczyły scamu w postaci typowego oszustwa phishingowego (45 vs 37%).

Osoby z podstawowym wykształceniem zdecydowanie częściej doświadczyły scamu w postaci fałszywego konkursu lub loterii (58 vs 38%), fałszywej akcji dobroczynnej (28 vs 17%).

Anna Goławska

Dyrektor ds. cyberbezpieczeństwa, Fujitsu Technology Solutions

Świadomość związana z bezpieczeństwem w internecie, jak również z możliwością cyberataków oraz ich rodzajami podnosi się z roku na rok na całym świecie, w tym również w Polsce. Czy świadomość Polek i Polaków jest już jednak wystarczająca?

Zgodnie z przeprowadzonym badaniem około 41% Polaków ocenia ryzyko związane z cyberatakiem jako wysokie lub bardzo wysokie. Pokazuje to, że jeszcze sporo osób nie zdaje sobie sprawy, że każdy z nas może stać się celem cyberataku.

Opierając się również na danych CERT Polska, można zauważyć, że faktycznie ryzyko cyberataku w Polsce jest wysokie, a w szczególności dotyczy to osób prywatnych. W Polsce, tak jak na całym świecie, liczba ataków zwiększa się z roku na rok. Znaczący wzrost można było zaobserwować w momencie wybuchu pandemii wirusa SARS-CoV-2, jak również po wybuchu pełnoskalowej wojny w Ukrainie.

Warto ponadto zwrócić uwagę, że w ubiegłym roku tylko w Polsce zanotowano 400 000 zgłoszeń z podejrzeniem cyberataku, obejmujących m.in ataki ransomware, DDoS, kampanie phishingowe mające na celu wyłudzanie danych, np. za pomocą fałszywych ankiet, e-maili zawierających linki do nieprawdziwych ofert inwestycyjnych i wiele innych. W bieżącym roku utrzymuje się tendencja wzrostowa.

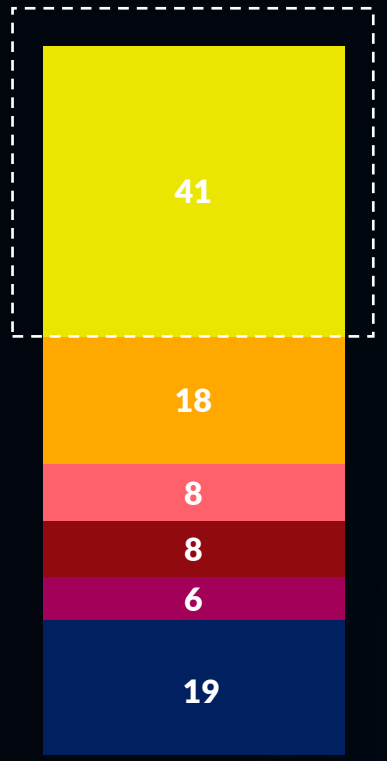
Zgodnie z ankietą aż 36% respondentów deklaruje, że miało styczność z incydentami cyberbezpieczeństwa, w tym więcej mężczyzn niż kobiet, najwięcej incydentów zadeklarowały osoby między 40. a 49. rokiem życia.

Osoby ankietowane wskazują również, że najczęstsze incydenty wiązały się z otrzymaniem fałszywego e-maila czy SMS-a (phishing), fałszywej reklamy, informacji o loterii itp. (scam) czy bezpośrednim kontaktem przez osobę podszywającą się pod kogoś innego (spoofing).

To pokazuje, że wciąż najsłabszym punktem, który jest wykorzystywany przez cyberprzestępców, jest człowiek. Posiadanie zaawansowanych technologii ochrony infrastruktury IT na pewno znacząco zmniejsza ryzyko ataku, trzeba jednak pamiętać o tym, że każdy z nas może popełnić błąd, a techniki stosowane przez cyberprzestępców, włączając w to techniki socjotechniczne, są coraz bardziej zaawansowane.

W związku z tym niezwykle ważne jest budowanie świadomości na temat zagrożeń, między innymi o tym, czym są cyberataki, jak można rozpoznać np. fałszywe strony, e-maile czy reklamy oraz promować dobre praktyki rozwiązań pozwalających na zabezpieczenie urządzeń, których używamy na co dzień.

Jak zmieniła się skala scamu w perspektywie ostatnich lat?



ROŚNIE OD 10 LAT 41%

♀ 36%	GenZ 38%	41%	32%
♂ 47%	Boomer 39%	39%	46%

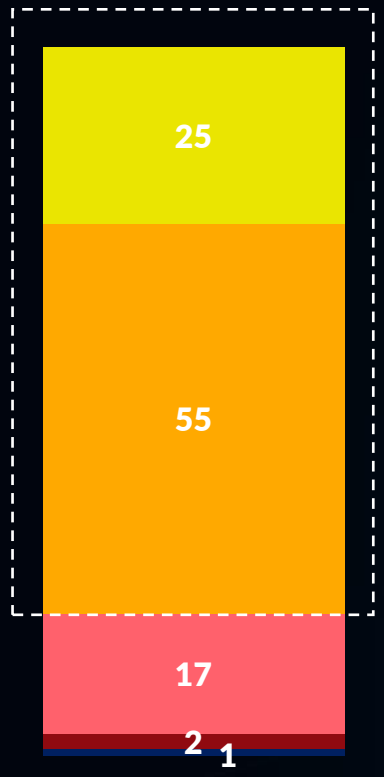
Jedynie 6% Polaków nie zaobserwowało wzrostu scamu.

4 na 10 uważa, że skala scamu rośnie nieprzerwanie, a 8%, że wzrosła najbardziej od czasu wojny w Ukrainie lub ChatGPT. Na pandemię, jako źródło wzrostu, wskazało 18%.

- Rośnie nieprzerwanie od 10 lat
- Wzrosła najbardziej od czasów COVID/Pandemii (2020)
- Wzrosła najbardziej od czasów wojny w Ukrainie (2022)
- Wzrosła najbardziej od czasów wprowadzenia ChatGPT (OpenAI, 2023)
- Nie zmienia się w ostatnich latach
- nie wiem / trudno powiedzieć

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Jak zmieni się skala scamu w perspektywie kolejnych pięciu lat?



8 na 10 Polaków uważa, że zjawisko scamu nasili się w kolejnych pięciu latach.

Zdecydowanie wzrośnie
Raczej wzrośnie
Nie zmieni się
Raczej zmaleje
Zdecydowanie zmaleje

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Konrad Płachecki

Dyrektor Biura Architektury i Systemów Cyberbezpieczeństwa, Bank Gospodarstwa Krajowego

Ponad 40% badanych ocenia na co najmniej wysokie ryzyko stania się ofiarą ataków i oszustw. Cyberataki, których jesteśmy ofiarą, mają coraz ciekawsze formy. Jesteśmy wręcz zalewani fałszywymi ogłoszeniami, konkursami, możliwościami szybkiego zysku. Co ciekawe, 20% badanych deklaruje, że przejęto ich konta w portalach internetowych. Niestety brakuje informacji, czy zawiodły zabezpieczenia samych portali, podatności w aplikacji, czy znaczenie miał brak funkcjonalności wieloskładnikowego uwierzytelniania, czy w wyniku ataku celowanego w użytkownika. Zaskakuje także piętnastoprocentowy poziom uczestnictwa badanych osób w atakach związanych z próbami szantażu i wymuszenia opłat. Może to być związane z częstymi wyciekami danych z portali i kompromitacją danych logowania ich użytkowników. O takich doświadczeniach napisało 11% badanych, co pokazuje, jak ważne jest śledzenie kompromitacji swoich danych logowania. Takie usługi wprowadziło już część przeglądarek internetowych i jest to coraz powszechniejsza usługa w programach chroniących stacje robocze. Tak więc chrońmy nasze hasła, nie udostępniajmy ich, stosujmy różne hasła do różnych portali, korzystajmy z portfeli haseł, dbajmy o ich odpowiednią długość i skomplikowanie.

Czarny rynek związany z cyberatakami nastawiony jest głównie na osiąganie w miarę prostych, ale dużych zysków. Jak pokazują wyniki badania, stosunkowo mało osób (4%) padło ofiarą ataku ransomware, który głównie celowany jest w organizacje mogące zapłacić godziwy okup, po wcześniejszym zinfiltrowaniu systemów i eksfoliacji wartościowych danych. Na takim działaniu skupiają się głównie zorganizowane grupy. Pojedyncze osoby padają ofiarą takich ataków przy pojawiających się powszechnych podatnościach, np. w systemach operacyjnych. Tutaj warto podkreślić, jak ważne jest posiadanie na stacji roboczej programu wykrywającego zagrożenia oraz zapewnienie stałej aktualizacji poprawek bezpieczeństwa w systemie operacyjnym.

Podsumowując, czynniki sprzyjające cyberprzestępczości, takie jak nieostrożność potencjalnych ofiar, nieodpowiednie zabezpieczenia czy brak wiedzy, zwiększają prawdopodobieństwo skutecznego przeprowadzenia na nich ataku, dlatego też edukacja odgrywa tutaj kluczową role. Umiejętność rozpoznania fałszywego maila lub zasada ograniczonego zaufania powinny towarzyszyć nam codziennie. Świat cyfrowy rozwija się dynamicznie, technologia jest integralną częścią naszej codzienności. Budujmy zatem naszą świadomość i edukujmy naszych znajomych i rodzinę, aby utrudnić cyberprzestępcom osiągnięcie celu.

Czynniki sprzyjające cyberprzestępczości z perspektywy konsumenta/obywatela

TOP 3

Nieostrożność ludzi (59%), nieodpowiednie zabezpieczenie systemów i urządzeń (48%) oraz brak wiedzy lub szkoleń (46%) są najczęstszymi czynnikami sprzyjającymi cyberprzestępczości z perspektywy konsumenta/obywatela.

Jedynie co piąty wskazał na brak pieniędzy.

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni częściej niż kobiety jako czynnik sprzyjający cyberprzestępczości wskazali na winę producenta, który zbyt mało uwagi poświęca cyberbezpieczeństwu (24 vs 14%) oraz brak kultury przestrzegania przepisów i polityk (30 vs 21%).

Panie częściej wskazały na nieodpowiednie zabezpieczenie systemów (51 vs 45%).

WIEK

Osoby starsze zdecydowanie częściej wskazały na następujące czynniki sprzyjające cyberprzestępczności:

- „Nieodpowiednie zabezpieczenie systemów i urządzeń" (62 vs 44%),
- „Wymagane jest ode mnie zbyt wiele kont, metod logowania, kanałów komunikacji" (34 vs 19%),
- „Cyberbezpieczeństwo to rola informatyków, a nie zwykłych ludzi" (27 vs 16%)
- oraz brak pieniędzy (27 vs 17%).

Osoby młodsze wskazały na rosnącą złożoność świata cyfrowego i brak intuicyjności inteligentnych rozwiązań z jakich korzystają (45 vs 22%).

MIEJSCE ZAMIESZKANIA

Osoby z dużych miast częściej wskazały na wymóg posiadania wielu kont czy metod logowania jako źródło czynników sprzyjających cyberprzestępczości (41 vs 31%). Osoby te również częściej wskazały na niefrasobliwości ludzi (66 vs 58%).

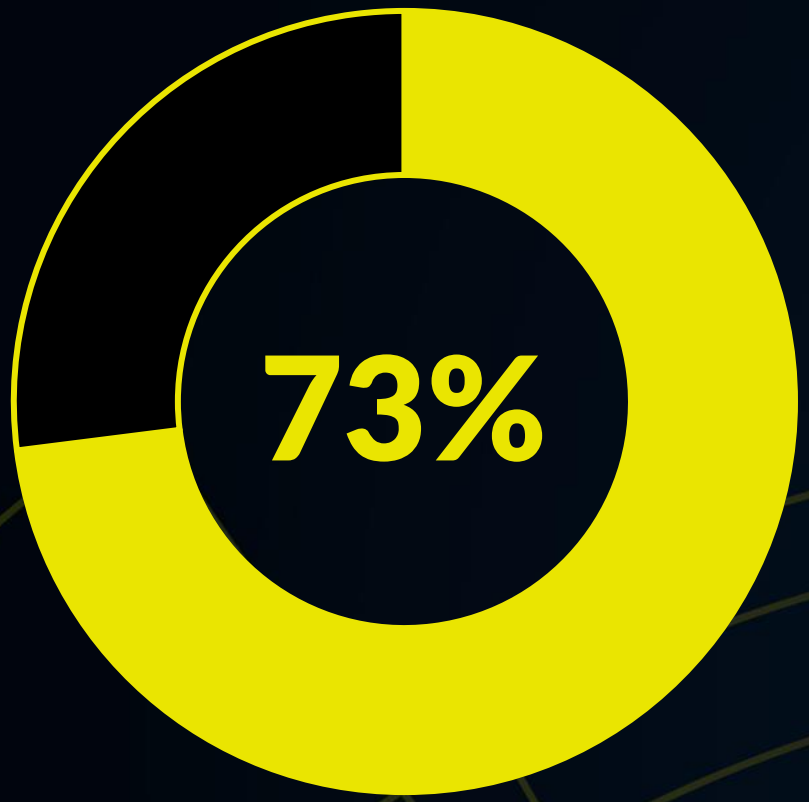
Osoby mieszkające na wsi częściej wskazały na rosnącą złożoność świata cyfrowego i brak intuicyjności inteligentnych rozwiązań z jakich korzy-stają (36 vs 28%).

WYKSZTAŁCENIE

Największe różnice zaobserwowano z punktu widzenia posiadanego wykształcenia.

Osoby z wyższym wykształceniem częściej wskazywały na rosnącą złożoność świata cyfrowego i brak intuicyjności inteligentnych rozwiązań z jakich korzystają (46 vs 21%), nieostrożności ludzi (65 vs 50%).

Osoby z wykształceniem podstawowym częściej wskazały, że cyberbezpieczeństwo to rola informatyków, a nie zwykłych ludzi (27 vs 14%).



7 na 10 Polaków chce uregulowania kar nakładanych na bigtech

w związku z oszustwami internetowymi.

W badaniu zapytano o konieczność uregulowania kar finansowych nakładanych na duże platformy internetowe takie jak Google Ads, TikTok, Facebook, Instagram, X w związku z brakiem lub powolnym czasem reakcji na oszustwa internetowe takie jak np. fałszywe reklamy.

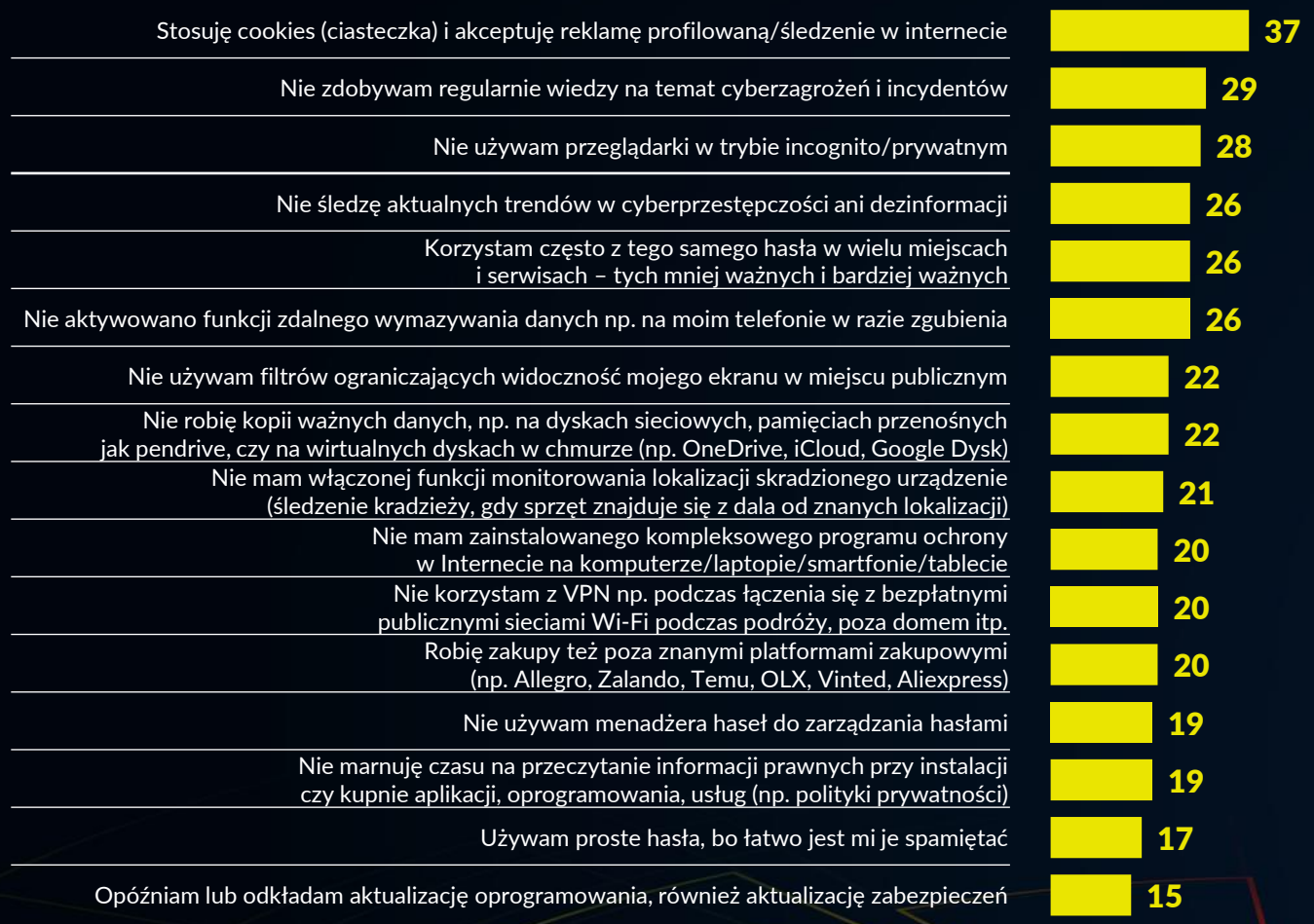
- ♀ 72%
- ♂ 74%
- GenZ 73%
- Boomer 74%
- 71%
- 85%
- 64%
- 82%

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

2.4.

Jakie mamy złe nawyki z zakresu cyberbezpieczeństwa?

Deklaratywna popularność złych nawyków z zakresu cyberbezpieczeństwa (1)



Co piąty Polak deklaruje czternaście z trzydziestu trzech badanych złych nawyków.

Nadal co czwarty Polak używa tego samego hasła w wielu miejscach i serwisach.

Do najbardziej popularnych nawyków można zaliczyć stosowanie profilowanej reklamy, brak zdobywania wiedzy o cyberzagrożeniach, niekorzystanie z przeglądarki w trybie prywatnym, czy brak śledzenia aktualnych trendów o dezinformacji czy cyberprzestępczości.

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Deklaratywna popularność złych nawyków z zakresu cyberbezpieczeństwa (2)

Mniej niż 10% Polaków deklaruje otwieranie załączników z e-maili pochodzących z niezaufanych źródeł, brak kasowania swoich danych z elektroniki w momencie sprzedaży czy wynajmu, klikania w linki bez patrzenia na szczegółowy adres nadawcy czy wykorzystania sprzętu służbowego do celów prywatnych.

Na bazie naszego testu i innych odpowiedzi można śmiało wskazać, że **popularność złych nawyków w rzeczywistości jest zaniżona i głównie deklaratywna.**

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Panowie częściej niż kobiety deklarowali pobieranie gier i aplikacji z niezaufanych źródeł (20 vs 9%), stosowanie ciasteczek (40 vs 34%) czy brak poczucia odpowiedzialności za cyberbezpieczeństwo w moim otoczeniu (12 vs 7%).

Panie zdecydowanie częściej wskazały, że nie zdobywają regularnie wiedzy na temat cyberzagrożeń czy incydentów (34 vs 23%), nie aktywowały funkcji zdalnego wymazywania danych na telefonie w razie jego zgubienia (31 vs 21%) oraz rzadziej śledzą trendy z zakresu cyberprzestępczości (30 vs 23).

WIEK

Osoby młodsze częściej deklarowały złe nawyki z zakresu cyberbezpieczeństwa. Dla ponad dziesięciu przypadków skala odpowiedzi wyniosła ponad dziesięć punktów procentowych.

Młode osoby znacznie częściej niż osoby starsze deklarowały korzystanie z ciasteczek (51 vs 29%), brak czytania informacji prawnych przy instalacji oprogramowania lub usługi (29 vs 10%), brak korzystania z przeglądarki w trybie prywatnym (36 vs 21%), opóźnianie instalacji aktualizacji oprogramowania (22 vs 7%), korzystanie z tego samego hasła w wielu serwisach (37 vs 22%) czy niekorzystanie z kompleksowego programu antywirusowego (27 vs 13%).

Osoby starsze częściej deklarowały brak zdobywania regularnie wiedzy na temat cyberzagrożeń i incydentów (37 vs 22%).

MIEJSCE ZAMIESZKANIA

Osoby z dużych miejscowości częściej zadeklarowały, że nie aktywowały funkcji zdalnego wymazywania danych na telefonie (37 vs 24%), nie mają włączonej funkcji monitorowania lokalizacji sprzętu w razie kradzieży (29 vs 19%).

Osoby mieszkające na wsi częściej deklarowały brak zdobywania wiedzy (33 vs 22%) czy nieczytanie informacji prawnych przy instalacji gry, usługi czy aplikacji (21 vs 15%).

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem częściej zadeklarowały brak włączonej funkcji monitorowania lokalizacji sprzętu w razie kradzieży (29 vs 12%), brak zdalnego wymazywania danych z urządzeń elektronicznych (32 vs 17%) czy brak robienia kopii danych w chmurze (26 vs 11%) i korzystanie ze sprzętu służbowego do spraw prywatnych (17 vs 3%).

Osoby z wykształceniem podstawowym częściej deklarowały brak zainstalowanego kompleksowego oprogramowania do ochrony w internecie (31 vs 23%).

Piotr Konieczny

Założyciel Niebezpiecznik.pl i autor cyklu wykładów „Jak nie dać się zhackować?”

Mądry Polak po szkodzie. To zdanie dobrze pasuje do wyników ankiety, a zwłaszcza odpowiedzi na trzy pytania: o braku przygotowania się na kradzież sprzętu, tj. niewłączenia opcji zdalnego namierzania lub wymazywania danych po jego utracie, o braku sporządzania kopii zapasowych i o nieaplikowaniu poprawek bezpieczeństwa.

Nie dziwi mnie natomiast to, że większość ankietowanych korzysta z ciasteczek, bo... ciężko z nich nie korzystać. Co może niektórych zdziwić, mnie – jako osoby z branży cyberbezpieczeństwa – mniej zależy na tym, aby ludzie blokowali ciasteczka czy skrypty, które ich profilują pod kątem reklamowym, a bardziej na tym, żeby zrozumieli zasadę ich działania. Te rozwiązania można bowiem sprytnie wykorzystać na swoją korzyść, np. po to, aby widzieć więcej produktów w niszy, którą zgłębiamy, lub taniej nabyć usługę, która nas interesuje, żerując na tzw. remarketingu. Wystarczy przerwać proces rezerwacji pokoju w hotelu na jednym z ostatnich kroków, a następnie obserwować reklamy z rabatami zachęcającym do rezerwacji noclegu w tym właśnie obiekcie, które pojawią się w mediach społecznościowych.

Jestem zaskoczony, że pomimo tak wielu wycieków danych, nagłaśnianych nie tylko przez media branżowe, lecz także mainstreamowe, wciąż tak wielu Polaków korzysta z tego samego hasła w więcej niż jednym ważnym dla nich serwisie i nie włącza dwuskładnikowego uwierzytelnienia. To znaczy, że rady, które pojawiają się praktycznie w każdym artykule dotyczącym wycieku danych, zupełnie nie trafiają do społeczeństwa. Cieszę się jednak, że edukacja w tym zakresie prowadzona jest nie tylko przez media, lecz także przez pracodawców w ramach organizowanych dla pracowników szkoleń z cyberbezpieczeństwa. Ze swojego trenerskiego doświadczenia wiem, że warto podczas takich szkoleń przekazywać rady nie tylko dotyczące bezpieczeństwa służbowego, lecz także prywatnego.

Fundamentalnie natomiast nie zgadzam się z sugestiami, które zostały zawarte w kilku pytaniach: że korzystanie z VPN w przypadku publicznych sieci Wi-Fi istotnie podnosi nasze bezpieczeństwo, że samo korzystanie z takich sieci jest istotnym zagrożeniem albo że ukrywanie domowego SSID ma jakiekolwiek znaczenie.

Wniosek jest jeden: jak widać, wciąż trzeba edukować w temacie cyberbezpieczeństwa. Wszystkich.

Robert Pławiak

Chief Digital and Information Officer (CDIO), Polpharma

Michał Kielczyk

Chief Security Officer (CSO), Polpharma

Na podstawie wyników badania dotyczącego nawyków Polaków w zakresie cyberbezpieczeństwa wyłania się obraz, który wymaga poważnej refleksji. Wyniki pokazują, że znaczna część polskiego społeczeństwa nie stosuje podstawowych praktyk bezpieczeństwa w sieci, co naraża ich na różnego rodzaju zagrożenia. W szczególności aż 37% badanych akceptuje śledzenie w internecie i stosowanie reklam profilowanych, a 29% przyznaje, że nie zdobywa regularnie wiedzy na temat cyberzagrożeń. Równie niepokojące jest to, że 26% korzysta z tych samych haseł w różnych serwisach, co zwiększa ryzyko kompromitacji kont w przypadku wycieku danych z jednej z tych platform.

Zachowania te są nie tylko wynikiem braku wiedzy, lecz także braku ustawicznego procesu edukacji i budowania świadomości wśród użytkowników. Tylko 10% badanych brało udział w kampaniach edukacyjnych na temat cyberbezpieczeństwa, a większość zdobywa wiedzę na własną rękę. Zaledwie 27% uczestniczyło w szkoleniach zorganizowanych przez pracodawców, co pokazuje, że firmy i instytucje mogą odegrać większą rolę w edukacji swoich pracowników.

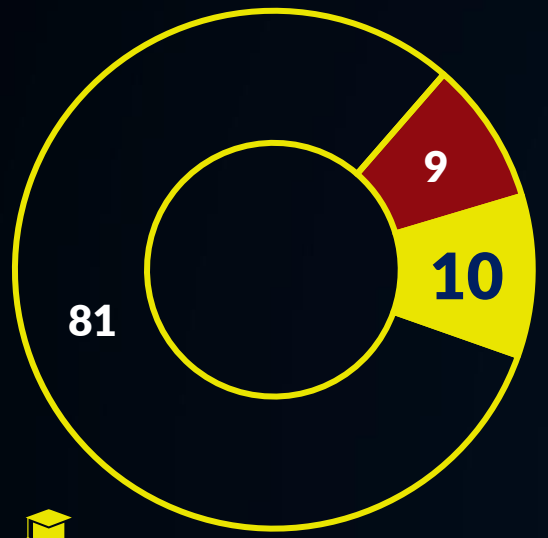
Z badań wynika również, że Polacy rzadko stosują zaawansowane środki ochrony, takie jak VPN czy dwuskładnikowe uwierzytelnianie, co mogłoby znacząco podnieść ich poziom bezpieczeństwa w sieci. Ponadto opóźnianie aktualizacji oprogramowania (15%) czy korzystanie z publicznych sieci Wi-Fi do operacji finansowych (12%) to kolejne alarmujące praktyki, które wskazują na brak zrozumienia zagrożeń.

Jedną z przyczyn takiego stanu rzeczy może być przeświadczenie użytkowników (nie tylko Polskich), że przecież nie będą celem ataku i im się to nie przydarzy. Podejście takie jest głównym hamulcem (poza przeświadczeniem o zbyt dużym poziomie trudności zagadnienia) w uzyskaniu zaangażowania i uwagi użytkowników w zmianę nawyków i zachowań. Warto skupić się na tych aspektach budowania świadomości, które pomogą odblokować u użytkowników chęć i potrzebę przyswajania nowej wiedzy.

Z perspektywy ekspertów ds. cyberbezpieczeństwa nadal niezmiennie kluczowe jest zintensyfikowanie działań edukacyjnych skierowanych zarówno do użytkowników indywidualnych, jak i firm oraz demonstrowanie zachowań wzmacniających edukację w tym obszarze. Wzrost świadomości i dostęp do informacji na temat cyberzagrożeń mogą znacząco zmniejszyć ryzyko ataków, a promowanie prostych zasad bezpieczeństwa, takich jak regularne zmiany haseł, stosowanie dwuskładnikowego uwierzytelniania czy regularne aktualizacje oprogramowania, powinno stać się priorytetem. Dodatkowo konieczne jest większe zaangażowanie instytucji państwowych i prywatnych w organizowanie kampanii edukacyjnych, które pomogą użytkownikom zrozumieć, jak ważna jest odpowiedzialność za własne bezpieczeństwo w sieci. Istotne jest, aby w dobie wszechobecnej sztucznej inteligencji (AI) wskazywać mocno na podstawowe nawyki, zachowania, które będą nas chronić.

Uczestniczenie w kampanii zwiększającej świadomość i wiedzę na temat cyberbezpieczeństwa

8 na 10 Polaków nie uczestniczyło w żadnej kampanii



♀ 8% ♂ 12%

GenZ 16% Boomer 4%

7% 7%

11% 9%

Tak
Nie wiem
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Gdzie lub jak uczestniczono w kampaniach?

Pytanie wielokrotnego wyboru
Baza: respondenci którzy uczestniczyli w kampanii (N=97)

PŁEĆ

Mężczyźni częściej niż kobiety deklarowali, że sami się dokształcają (49 vs 32%).

Kobiety częściej niż mężczyźni brały udział w kampaniach rządowych, spotach emitowanych w mediach.

WIEK

Osoby starsze częściej od osób młodszych deklarowały, że same się dokształcają (51 vs 37%) czy brały udział w kampaniach rządowych, spotach emitowanych w mediach (24 vs 10).

Osoby młode zadeklarowały, że częściej w inny sposób brały udział w kampaniach niż wyszczególniono w badaniu (20 vs 9%).

MIEJSCE ZAMIESZKANIA

Osoby mieszkające w dużych miastach częściej deklarowały udział w kampaniach organizowanych przez firmy (25 vs 11%), z kolei aż o 23 punkty procentowe osoby na wsiach deklarowały udział w kampaniach rządowych czy spotach emitowanych w mediach (23 vs 0%).

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem znacząco częściej deklarowały udział w szkoleniach realizowanych przez pracodawców (45 vs 1%) czy że same się dokształcają (36 vs 10%).

Osoby z podstawowym wykształceniem częściej deklarowały udział w kampaniach rządowych czy spotach emitowanych w mediach (28 vs 6%).

dr inż. Elżbieta Andrukiewicz

Kierownik Zakładu Cyberbezpieczeństwa, Instytut Łączności – Państwowy Instytut Badawczy, ekspert normalizacyjny

Badanie przeprowadzone w sierpniu 2024 na reprezentatywnej próbce Polek i Polaków dotyczyło cyberbezpieczeństwa i postrzegania zagrożeń, jakie w sobie niesie coraz powszechniejsze korzystanie z możliwości cyberprzestrzeni do realizacji czynności dnia codziennego.

Badanie obejmowało szerokie spektrum zagadnień, koncentrując się jednak na specyficznej kategorii zagrożeń, jaką jest cyberprzestępczość i oszustwa internetowe. Nie ma w tym nic dziwnego, ponieważ schematy oszustw znane od wieków ewoluują współbieżnie z rozwojem technik informatycznych. Czy nazwane scamem, czy oszustwem, jest to działanie przestępcze, a nowość polega jedynie na zastosowanych narzędziach, przy czym istota przestępstwa pozostaje ta sama.

Z badań wynika, że kradzież tożsamości jest postrzegana przez respondentów jako największe zagrożenie w cyberprzestrzeni. Do technik powszechnie stosowanych przez oszustów internetowych, którzy mogą mieć na celu kradzież tożsamości, jest podstępne pozyskiwanie informacji, czyli phishing. Uzyskane informacje mogą prowadzić do jednorazowego podszywania się pod autoryzowanego użytkownika, aby przykładowo skorzystać z jego zasobów finansowych, albo wręcz do kradzieży tożsamości, co może prowadzić do całkowitego przejęcia kontroli przez oszusta nad życiem jego internetowej ofiary.

Jakkolwiek korzystanie z serwisów, w których zagrożenie kradzieżą tożsamości występuje, np. z usług bankowości internetowej lub zakupów online, większość respondentów uważa za mało bezpieczne, to czynnik wygody i skuteczności przeważa. Co może napawać niepokojem, to fakt, że znaczny odsetek respondentów doświadczył oszustw internetowych na własnej skórze. Co piąty ankietowany stwierdził, że zostało przejęte jego konto w mediach społecznościowych, sklepie internetowym, forum itp. Nie zostało zadane pytanie, jaką faktyczną szkodę taka osoba poniosła (czy wymierną, finansową, czy innego typu np. utratę dobrego imienia w jakiejś społeczności), ale wskaźnik 20% jest alarmujący.

Warto zauważyć, że respondenci są świadomi zagrożeń i poszukują informacji, w jaki sposób można się zabezpieczyć. Dwie trzecie z nich, niezależnie od kategorii wiekowych, deklaruje chęć poszerzenia wiedzy o zagrożeniach w cyberprzestrzeni. Nie może być zaskoczeniem, że młodsze grupy ankietowanych już uważają się za osoby dobrze zaznajomione z technikami i sposobami oszustw internetowych i twierdzą, że potrafią rozpoznać próby tego rodzaju (ok. 1/3 respondentów w grupach wiekowych 19–29 oraz 30–39 lat). Jeśli tak faktycznie jest, warto profilować działania edukacyjne uwzględniając potrzeby oraz percepcję starszych grup użytkowników, aby minimalizować prawdopodobieństwo powodzenia internetowego odpowiednika metody oszustwa „na wnuczka”.

2.5.

Jak dbamy o bezpieczeństwo i przetwarzanie naszych danych?

Gdzie Polacy przechowują swoje cyfrowe dane takie jak zdjęcia, dokumenty, filmy, kontakty?

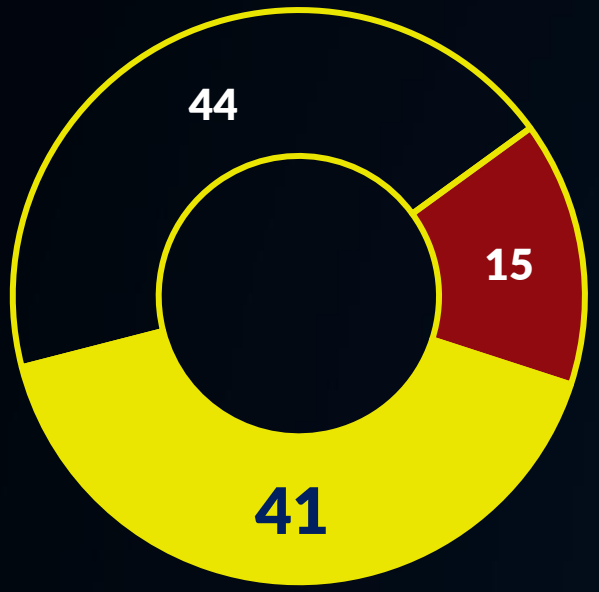
Co drugi Polak przechowuje dane na urządzeniach elektronicznych. Co trzeci na pamięciach przenośnych, a co czwarty w chmurze.

Jedynie 7% Polaków korzysta z dysków sieciowych.

Kobiety częściej drukują dokumenty (16 vs 7%), a młodzi częściej niż starsze osoby trzymają dane w chmurze (33 vs 16%).

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Czy Polacy wykonują kopie bezpieczeństwa kluczowych danych (tzw. backup)?



6 na 10 Polaków nie wykonuje, lub nie wie czy wykonuje zapasową kopię swoich kluczowych danych.

♀	37%	GenZ	46%		41%		41%
♂	44%	Boomer	33%		37%		50%

Tak
Nie wiem
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Robert Zyskowski

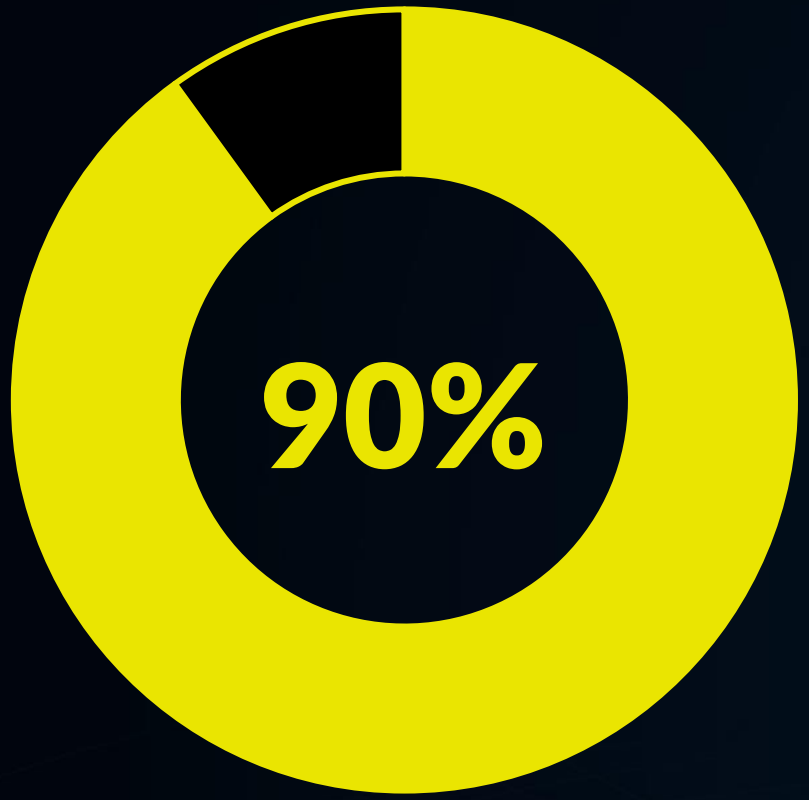
Członek zarządu, dyrektor ds. technologii (CTO), Symfonia

Zawsze cieszyła mnie możliwość skonfrontowania tzw. obiegowych opinii lub własnych poglądów z twardymi danymi. Traktuję to jako znakomitą okazję do refleksji i weryfikacji moich przekonań, a nierzadko także powód do ich zmiany. Tym razem, poszukując wiarygodnych informacji na temat przechowywania danych cyfrowych, sięgnąłem po bardzo ciekawy raport fundacji Digital Poland, poświęcony cyberbezpieczeństwu.

Podczas analizy danych w nim zgromadzonych bardzo ucieszył mnie znaczny poziom zaufania do przechowywania danych w chmurze, deklarowany przez 24% respondentów biorących udział w badaniu. Gorzej wypada tworzenie papierowych kopii, pozostające niestety na poziomie powyżej 10%. Wskazuje to na występującą przestrzeń do dalszej cyfryzacji naszego społeczeństwa. Przy okazji warto zwrócić uwagę, że wykonywanie kopii bezpieczeństwa kluczowych danych ciągle pozostawia wiele do życzenia, ponieważ 44% respondentów odpowiedziało, że tego typu kopii w ogóle nie wykonuje. Wartość ta rośnie wraz z wiekiem respondentów, sięgając nawet 54% w najstarszej kategorii wiekowej. Innym godnym zauważenia faktem jest praktycznie takie samo traktowanie komputerów stacjonarnych czy laptopów oraz urządzeń mobilnych, takich jak smartfony i tablety. Stawia to ciekawe wyzwania przed działami IT i bezpieczeństwa danych w przedsiębiorstwach. Wszyscy przyzwyczailiśmy się, że służbowy komputer czy laptop podlega nadzorowi i ochronie zapewnianej przez politykę bezpieczeństwa opracowaną przez dział IT. Jednocześnie powszechne zjawisko używania służbowych smartfonów bądź tabletów do celów prywatnych i na odwrót, prywatnych do celów służbowych, przysparza o ból głowy niejednego szafa działu IT i firmowego prawnika.

Ciekawą obserwacją wynikającą z raportu jest wpływ świadomości istnienia Rozporządzenia o Ochronie Danych Osobowych (RODO) na poczucie bezpieczeństwa w zakresie prywatności danych osobowych. Okazuje się, że bardzo wysoki poziom świadomości obowiązków wynikających z RODO, na poziomie 90%, przekłada się w stosunkowo niewielki sposób na zwiększenie poczucia bezpieczeństwa w zakresie prywatności danych osobowych i ich przetwarzania. Tylko 12% respondentów zadeklarowało, że RODO w zdecydowany sposób przyczyniło się do zwiększenia tego poczucia, podczas gdy 37% twierdzi, że wcale lub raczej nie. Ponadto, zdaniem respondentów, Polacy ciągle dość niefrasobliwie zostawiają swoje dane osobowe w różnych miejscach, np. w formularzach internetowych, sklepach itp.

Prawie wszyscy Polacy słyszeli o Rozporządzeniu o Ochronie Danych Osobowych (RODO)



DEFINICJA RODO DLA RESPONDENTA*

Rozporządzenie o Ochronie Danych Osobowych (RODO)

- chroni osoby fizyczne w związku z przetwarzaniem ich danych przez podmioty prywatne oraz przez większość podmiotów publicznych;
- umożliwia ono osobom fizycznym lepszą kontrolę nad ich danymi osobowymi. Zapewnia modernizację i ujednolicenie przepisów, umożliwiając przedsiębiorstwom ograniczenie biurokracji i korzystanie ze zwiększonego zaufania klientów;
- ustanawia ono całkowicie niezależne organy nadzorcze odpowiedzialne za monitorowanie stosowania i egzekwowanie przestrzegania przepisów.

Źródło: EUR-Lex

* pytanie zadano po podaniu definicji

♀ 92%
♂ 89%

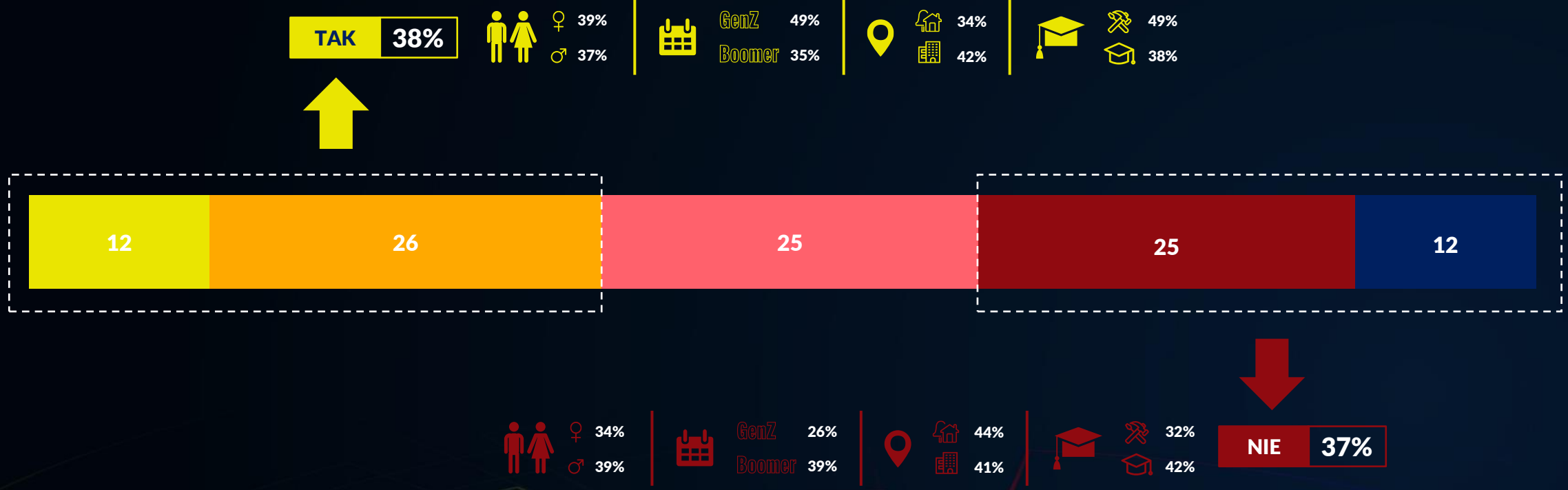
GenZ 88%
Boomer 91%

90%
93%

83%
92%

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Czy wprowadzenie RODO zwiększyło poczucie bezpieczeństwa w zakresie prywatności danych osobowych i ich przetwarzania?



Pytanie jednokrotnego wyboru
Baza: respondenci którzy słyszeli o RODO (N=904)

dr Urszula Góral

Adiunkt w Instytucie Nauk o Polityce i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego, przez ponad 15 lat pełniła funkcję dyrektora Departamentu Współpracy Międzynarodowej i Edukacji w Urzędzie Ochrony Danych Osobowych (wcześniej GIODO), obecnie pracuje jako inspektor ochrony danych w Kancelarii Sejmu Rzeczypospolitej Polskiej.

Wyniki badań pokazują, że ponad 90% ankietowanych jest świadomych obowiązywania przepisów rozporządzenia ogólnego o ochronie danych osobowych. Jest to wynik, który pozwala stwierdzić, że obowiązywanie RODO na dobre utrwaliło się w świadomości Polaków.

Nie jest on zaskoczeniem, ponieważ w przestrzeni publicznej obowiązywanie RODO utrwaliło się w ciągu ostatnich lat, choć samo poznanie RODO oznaczać będzie raczej przekonanie o istniejącym zestawie praw, zasad i obowiązków niż ich szczegółową znajomość. Wiele prowadzonych kampanii edukacyjnych, w tym działania UODO – organu ochrony danych z ponad dwudziestopięcioletnią tradycją – znacząco przyczyniło się do wzrostu świadomości zarówno wśród osób fizycznych, jak i przedstawicieli biznesu. Nie bez znaczenia są akcje informacyjne, w które angażują się organizacje społeczne. Wszystkie te aktywności przez ostanie lata były ukierunkowane na wzmocnienie obowiązywania przepisów o ochronie danych osobowych, ich skutecznego stosowania i egzekwowania na co dzień.

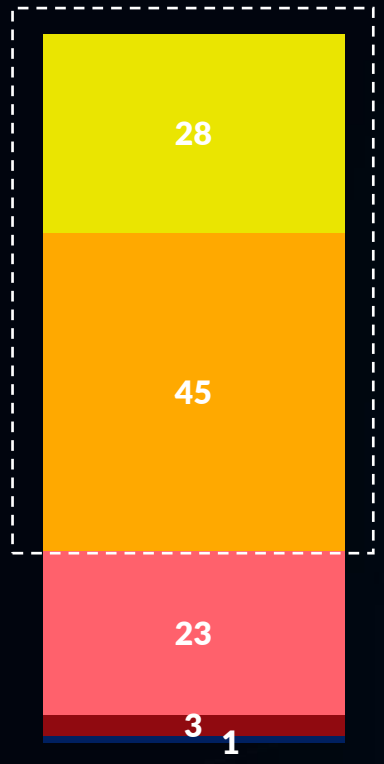
RODO to akt prawny, który sposób jednolity ma zagwarantować spójne stosowanie przepisów o ochronie danych w całej UE. I wydaje się, że Polacy, którzy chętnie podróżują za granicę turystycznie, ale też prowadzą działalność gospodarczą również poza terytorium naszego kraju, doceniają obowiązywanie przepisów, które mają na celu zagwarantowanie swobodnego obiegu danych osobowych w obrębie rynku wewnętrznego UE, dostarczając jednolity system praw i obowiązków, bez względu na to w którym państwie UE przebywamy, studiujemy czy pracujemy.

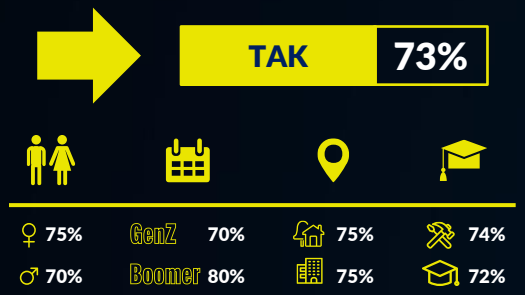
Biorąc pod uwagę wpływ nowych technologii na prawa i wolności osób fizycznych, w tym zwłaszcza rozwój systemów AI, świadomość obowiązywania tego aktu prawnego w niemal każdej dziedzinie swojego życia zwiększyło powszechną wiedzę na temat danych osobowych i świadomość konieczności ich ochrony.

Z odpowiedzi ankietowanych wynika, że brak jest jednoznacznego potwierdzenia, że wprowadzenie RODO znacząco wpłynęło na zwiększenie poczucia bezpieczeństwa w zakresie prywatności danych osobowych i ich przetwarzania. Mamy w tym przypadku sytuację, w której taka sama liczba osób wskazuje na poprawę bezpieczeństwa w odniesieniu do przetwarzania ich danych osobowych (zdecydowanie bądź w pewnym stopniu), jak osób, które uważają, że obowiązywanie RODO w żadne sposób nie wpłynęło na poprawę sytuacji w tym zakresie. Może to wiązać się z pewnym zjawiskiem, które wielokrotnie wskazywali eksperci od edukacji i prywatności a mianowicie braku przełożenia wiedzy i znajomości prawa, a także zagrożeń wynikających z naruszenia zasad, na właściwe postawy i zachowania, zarówno osób fizycznych (w tym również dzieci i młodzieży), jak i osób prawnych i innych podmiotów nieposiadających osobowości prawnej.

Analiza wyników odpowiedzi pokazuje, że w ocenie ankietowanych Polacy zbyt nieostrożnie zostawiają swoje dane osobowe w różnych miejscach, np. w formularzach internetowych, sklepach. Jest to w mojej opinii sygnał, że w tym kierunku należy prowadzić działania edukacyjne.

Czy Polacy zbyt nieostrożnie zostawiają swoje dane osobowe w różnych miejscach, np. w formularzach internetowych, sklepach?





7 na 10 badanych ocenia, że Polacy **zbyt nieostrożnie** zostawiają swoje dane osobowe w internecie.

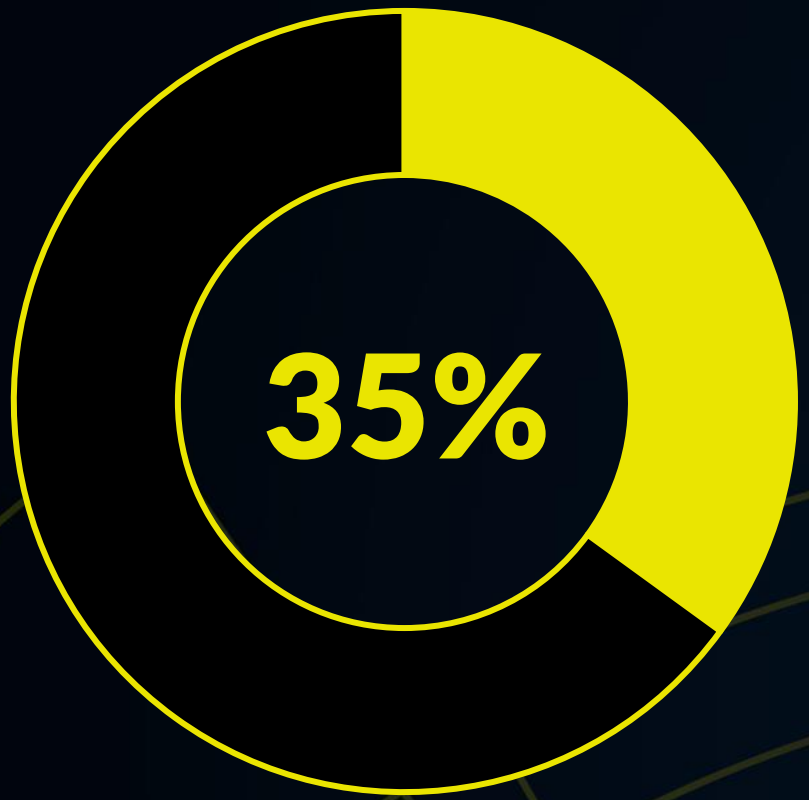
Zdecydowanie tak
Raczej tak
Nie wiem / nie mam zdania
Raczej nie
Zdecydowanie nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

2.6.

Czy doświadczamy mowy nienawiści i jak ją ograniczyć?

Co trzeci Polak osobiście doświadczył mowy nienawiści w sieci



DEFINICJA RODO DLA RESPONDENTA*

Według Europejskiej Komisji Przeciwko Rasizmowi i Nietolerancji (ECRI) - **mowa nienawiści** to dowolna forma komunikacji, która atakuje, szkaluje, oczernia lub podżega do przemocy lub dyskryminacji osób lub grup w oparciu o określone cechy, takie jak rasa, kolor skóry, pochodzenie etniczne, religia, płeć, orientacja seksualna, niepełnosprawność, czynnik tożsamości lub narodowość.

Ten rodzaj mowy ma na celu szerzenie nienawiści, promowanie nietolerancji i często przyczynia się do marginalizacji lub dehumanizacji grupy docelowej.

Podżeganie jest bardzo niebezpieczną formą wypowiedzi, ponieważ wyraźnie i celowo ma na celu wywołanie dyskryminacji, wrogości i przemocy, co może również prowadzić do terroryzmu lub okrutnych przestępstw.

Mowa nienawiści to także wszelkie nękanie, obrażanie, negatywne stereotypizowanie lub grożenie takiej osobie lub osobom oraz wszelkie usprawiedliwianie wszystkich tych form agresji.

* pytanie zadano po podaniu definicji

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Renata Gluza

Dziennikarka i redaktorka, w mediach od 1990 roku, zaczynała w PAP, potem pracowała w „Echu Krakowa", „Gazecie Wyborczej Kraków", „Press", „Forbes Women", od 2020 roku wydawca serwisu factcheckingowego Konkret24 w portalu Tvn24.pl, TVN Warner Bros. Discovery

Coraz łatwiejszy dostęp do internetu i poczucie (nie zawsze słuszne) własnej anonimowości powoduje, że w sieci ujawniają się patologiczne i złe skłonności jej użytkowników. W realu byłyby szybko napiętnowane czy wręcz karane, lecz w świecie wirtualnym zbierają ogromne żniwo. Mowa nienawiści (inaczej hejting) to zjawisko kulturowe, które bez internetu nie stałoby się tak powszechne. Jest produktem ubocznym cyfryzacji.

Jeśli więc mówimy dziś o bezpieczeństwie w internecie i zagrożeniach, trzeba brać pod uwagę również zdrowie psychiczne. Niepohamowywany strumień przekazów, które szkalują, oczerniają lub dyskryminują osoby z powodu ich wyglądu, rasy, pochodzenia, religii, płci, orientacji seksualnej, narodowości itd. wyrządza równie istotne szkody jak złośliwe oprogramowanie czy scamy. Budzi lęk, rujnuje poczucie bezpieczeństwa w sieci, prowadzi do kolejnych destrukcyjnych zachowań.

Jak wynika z niniejszego raportu, wielu z nas już to zauważa. Na pytanie, czy kiedykolwiek doświadczyli mowy nienawiści w internecie, 35% badanych Polaków odpowiedziało, że tak. Doświadczenie to bardziej dotyczy mężczyzn (42% pytanych odpowiedziało twierdząco) niż kobiet (28%).

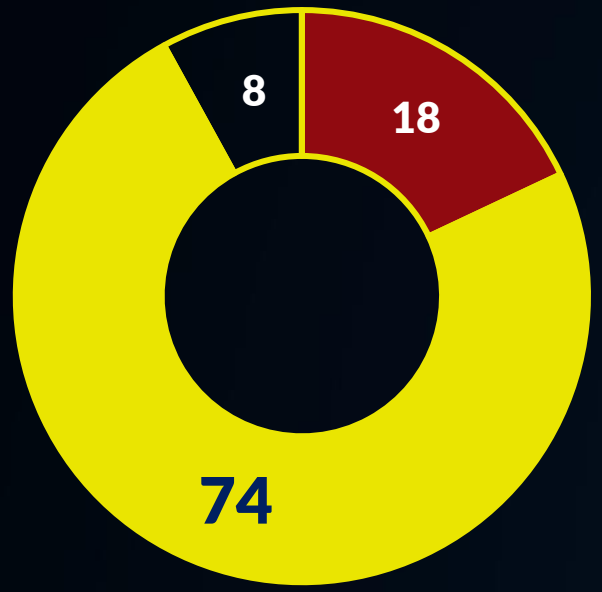
Zwróćmy też uwagę na wiek: otóż z mową nienawiści zetknęło się aż 50% respondentów będących w wieku 18–29 lat i aż 46% trzydziestolatków. Są to najwyższe wskaźniki, jeśli chodzi o grupy wiekowe. I bardzo niepokojące: młodzi ludzie zdają się być głównymi ofiarami hejtingu. Na pytanie, czy w internecie jest zbyt dużo mowy nienawiści, aż 81% badanych w grupie 18–19 lat odpowiedziało „tak".

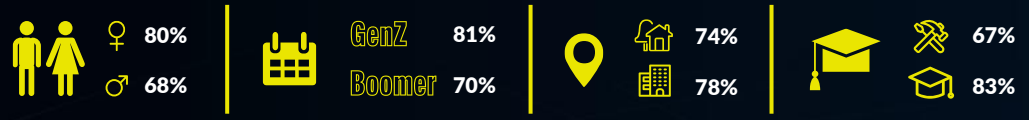
To oni spędzają dziś najwięcej czasu w mediach społecznościowych, są więc najbardziej nastawieni na działanie kolejnych wytworów hejtingu typu profile nienawiści (z ang. hate pages), czyli stron zakładanych na Facebooku bądź Instagramie, na których hejtuje się wybrane osoby czy grupy.

Zmęczenie szerzącą się w internecie mową nienawiści wyraża już większość jego użytkowników – 74% badanych Polaków twierdzi, że jest jej zbyt dużo. We wszystkich grupach wiekowych na pytanie, czy należy więc prawnie uregulować walkę z tym zjawiskiem, ok. 70% odpowiedziało, że tak. Z kolei 64% Polaków jest za tym, by wprowadzić tzw. ślepe pozwy w celu walki z anonimową agresją w postaci hejtu. Poczucie anonimowości powoduje bowiem, że atakujący słowem czują się bezkarni.

Jednak nie łudźmy się: złożony we wrześniu 2024 roku poselski projekt nowelizacji Kodeksu postępowania cywilnego, który dopuszcza składanie pozwów w sprawach o naruszenie dóbr osobistych przeciwko anonimowym internautom (zwany ustawą antyhejterską), to dopiero pierwszy mały krok w długim marszu prowadzącym do wyrugowania hejtu z internetowego ekosystemu.

Czy w sieci jest za dużo mowy nienawiści?



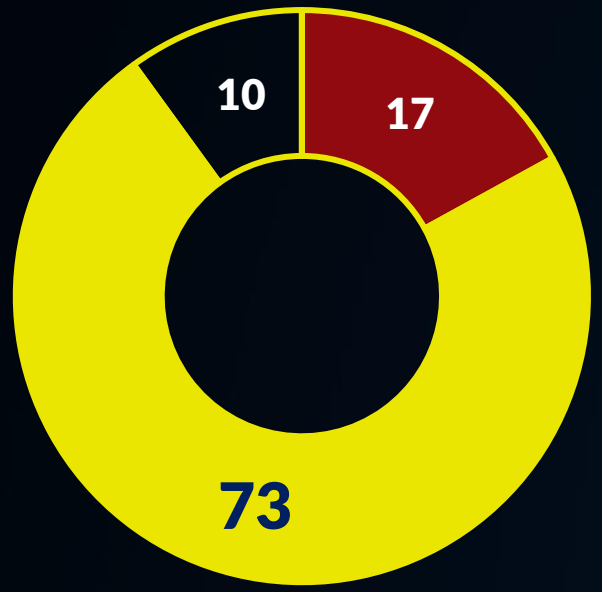


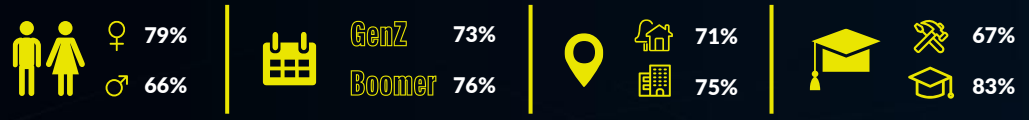
Ponad 7 na 10 Polaków uważa, że w sieci jest zbyt dużo mowy nienawiści.

Tak
Nie mam zdania
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Czy należy uregulować prawnie walkę z mową nienawiści i dokonać zmian w prawie?





Tak
Nie mam zdania
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Ponad 7 na 10 Polaków uważa, że należy dokonać **zmian w kodeksie karnym** i uregulować prawnie walkę z mową nienawiści, gdyż dziś np. **nie ma w nim definicji hejtu.**

Małgorzata Kilian-Grzegorczyk

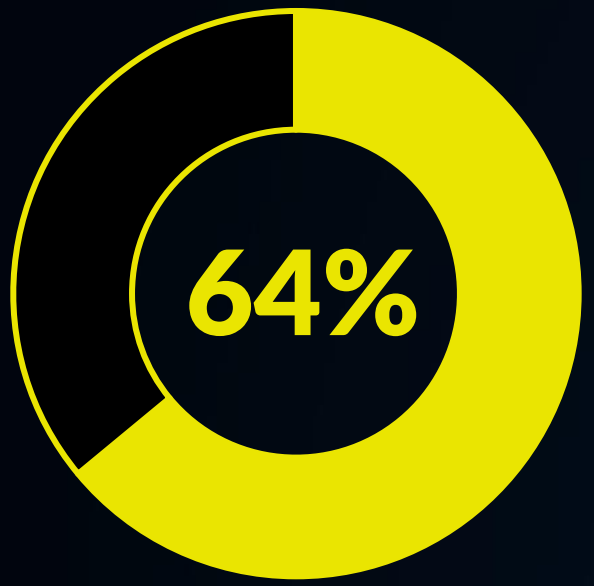
Prezeska Stowarzyszenia Demagog

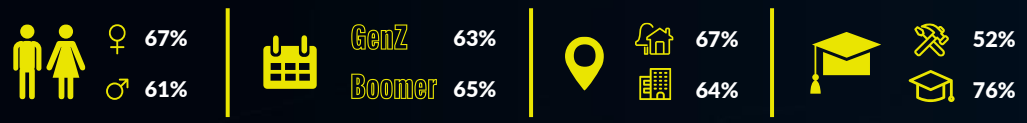
Mowa nienawiści w internecie to poważne zagrożenie dla poczucia bezpieczeństwa społeczeństwa, szczególnie w dobie rosnącej cyfryzacji i anonimowości w sieci. Z badania wynika, że aż 35% Polaków doświadczyło osobiście mowy nienawiści w sieci, co podkreśla skalę tego problemu. Tego typu doświadczenia mogą prowadzić do trwałych skutków psychologicznych, zwłaszcza u dzieci i nastolatków, takich jak obniżenie samooceny, stres czy lęk, a także sprzyjać dalszemu pogłębianiu podziałów społecznych.

Jednym z kluczowych czynników sprzyjających rozwojowi mowy nienawiści w internecie jest brak odpowiednich regulacji prawnych, które skutecznie zniechęcałyby do tego rodzaju zachowań. Wiele osób czuje się bezkarnie, korzystając z anonimowości, jaką daje internet, co zwiększa ich skłonność do przemocy słownej. Wyniki badania pokazują, że 73% Polaków popiera wprowadzenie zmian w prawie mających na celu walkę z mową nienawiści, co wskazuje na silną potrzebę społeczną w tym zakresie. Wprowadzenie do polskiego systemu prawnego instytucji tzw. ślepego pozwu, które wspiera 64% badanych, mogłoby znacząco utrudnić działania osób, które korzystają z anonimowości internetu w celu szerzenia nienawiści.

Polaryzacja społeczna oraz dezinformacja, które są coraz bardziej widoczne w Polsce, dodatkowo wzmacniają zjawisko mowy nienawiści. Dezinformacja sprzyja powstawaniu fałszywych narracji, które z kolei wywołują agresję wobec określonych grup społecznych czy osób. Polaryzacja prowadzi do eskalacji konfliktów między różnymi grupami, co sprzyja używaniu mowy nienawiści jako narzędzia walki ideologicznej. Z tego względu przeciwdziałanie mowie nienawiści powinno być priorytetem, a odpowiednie regulacje prawne są niezbędnym krokiem w tej walce.

Poparcie dla wprowadzenia do porządku prawnego tzw. ślepego pozwu





2 na 3 Polaków popiera wprowadzenie do porządku prawnego tzw. ślepego pozwu w celu walki z anonimowym hejtem w sieci.

DEFINICJA ŚLEPEGO POZWU DLA RESPONDENTA*

„Ślepy pozew” to termin używany w odniesieniu do pozwu złożonego bez znajomości przez powoda prawdziwej tożsamości pozwanego w momencie składania pozwu.

Dzieje się tak często w przypadkach, gdy powód zna pozwanego jedynie z nazwy użytkownika online (tzw, ksywka/nick/login), adresu IP lub innych pośrednich identyfikatorów. Nie posiada on jednak danych teleadresowych (np. adresu zamieszkania) i jego danych. Rolą sądów/organów państwa byłoby ustalenie tożsamości np. osoby łamiącej prawo w internecie.

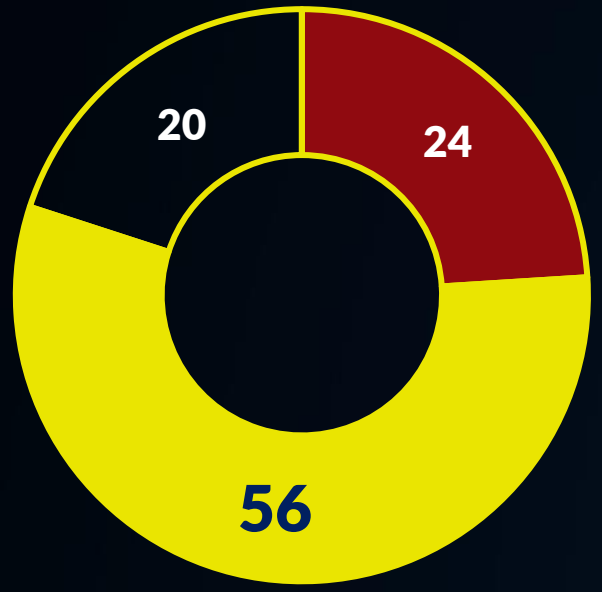
* pytanie zadano po podaniu definicji

ⓘ Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

2.7.

Jak zadbać o ochronę dzieci i młodzieży w Internecie?

Czy polskie prawo nie chroni odpowiednio dzieci przed treściami dla dorosłych w sieci?



♀ 60%
♂ 52%

GenZ 66%
Boomer 44%

53%
56%

57%
43%

Tak
Nie mam zdania
Nie

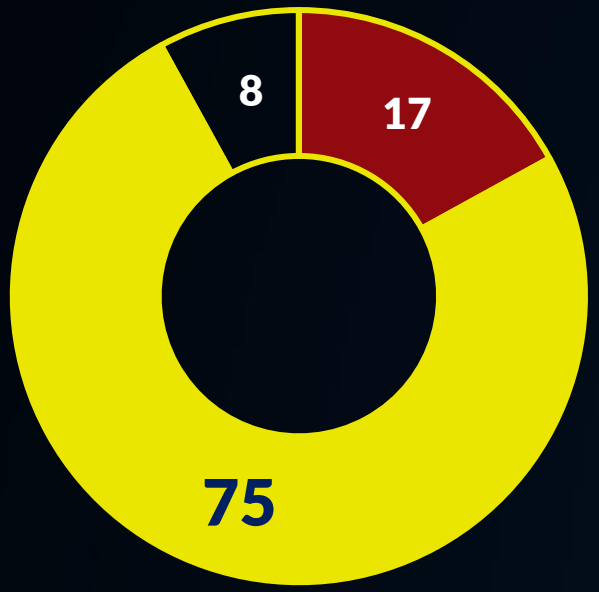
Ponad połowa Polaków uważa, że polskie prawo nie chroni dzieci przed treściami dla dorosłych* w sieci.

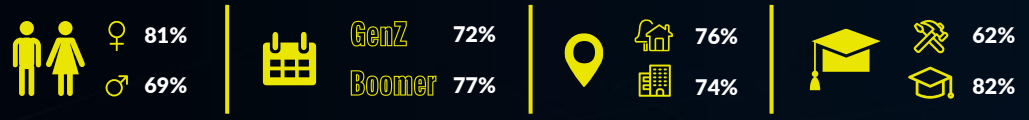
*treści dla dorosłych to np. strony porno, producentów alkoholi czy zakładów bukmacherskich. Dziś można wejść do serwisu z treściami pornograficznymi w internecie i samemu deklarować, że ma się 18 lat.

Z odpowiedzią zgadzały się bardziej osoby będące bardziej aktywne w internecie (69 vs 52%, gdzie 69% dotyczy osób o zbyt dużej ilości kont w internecie, a 52% małej), w większych gospodarstwach domowych (67 vs 49% gdzie 67% dotyczy gospodarstw w których jest minimum 4 osoby, a 49% dotyczy jednoosobowych gospodarstw domowych), posiadające dzieci (63 vs 53%).

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Czy to co jest zabronione w świecie rzeczywistym powinno być też zabronione i przestrzegane w sieci?





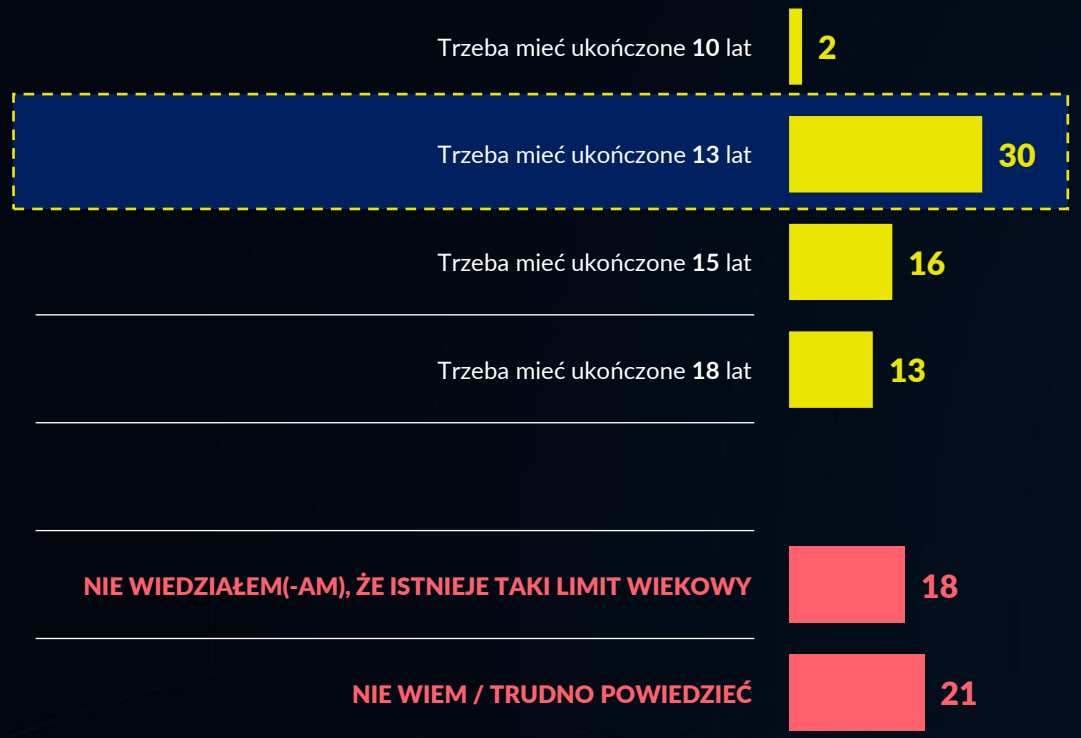
3 na 4 Polaków uważa, że to co jest zabronione w świecie rzeczywistym powinno być **też zabronione i przestrzegane w sieci.**

Pytanie: Czy uważa Pan(i), że to co jest zabronione w świecie rzeczywistym/fizycznym (np. zakaz sprzedaży alkoholu/energetyków/treści pornograficznych dzieciom w sklepie) powinno być też zabronione i przestrzegane w internecie? (np. zakaz dostępu dla dzieci do treści porno przez internet, zakaz możliwości kupna alkoholu przez dzieci przez internet)?

Tak
Nie mam zdania
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Test wiedzy z minimalnego legalnego wieku umożliwiającego założenie konta w mediach społecznościowych



Jedynie 3 na 10 Polaków poprawnie odpowiedziało na pytanie dotyczące minimalnego wieku uprawniającego do założenia konta.

Co piąty nie wiedział, że istnieje w ogóle taki limit.

Pytanie: Od którego roku życia można legalnie utworzyć konto na mediach społecznościowych takich jak Facebook, Instagram, Tiktok, Snapchat, YouTube?

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Kobiet częściej niż mężczyźni wskazały poprawną odpowiedź w teście z minimalnego wymaganego wieku pozwalającego na założenie konta w mediach społecznościowych (34 vs 26%).

Sumując wszystkie pozostałe błędne odpowiedzi to mężczyźni częściej nie mieli wiedzy o wieku uprawniającym do skorzystania z mediów społecznościowych wynoszącym 13 lat (74 vs 66%).

WIEK

Młodzi ludzie mieli zdecydowanie lepszą wiedzę na temat minimalnego wymaganego wieku uprawniającego do skorzystania z mediów społecznościowych (61 vs 7%).

Osoby starsze albo błędnie wskazały inne odpowiedzi (wiek 10, 15, 18 lat) albo wskazały, że nie wiedziały, że taki limit w ogóle istnieje.

Sumaryczna odpowiedź błędnych odpowiedzi dla osób starszych w porównaniu błędnymi odpowiedziami osób młodych wynosi 93 do 39%.

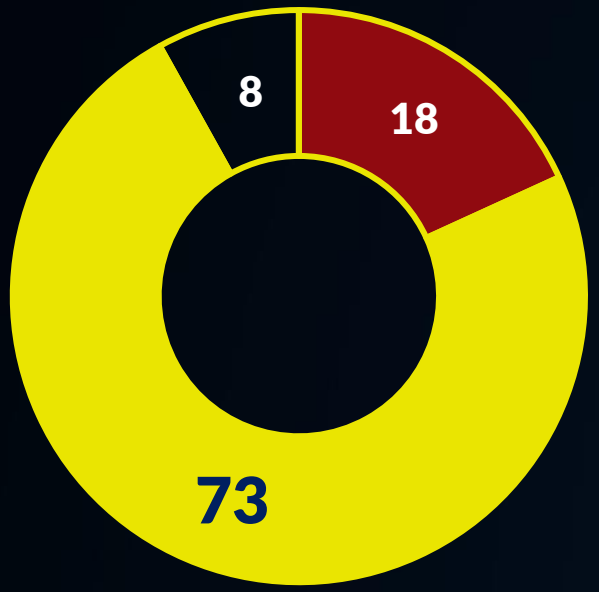
MIEJSCE ZAMIESZKANIA

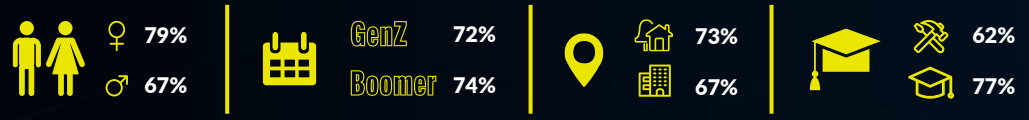
Miejsce zamieszkania nie różnicowało wskazania błędnej lub poprawnej odpowiedzi, a wskazania poprawnych lub błędnych odpowiedzi różnią się jedynie pojedynczymi punktami procentowymi.

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem częściej od osób z wykształceniem podstawowym wskazały na poprawną odpowiedź (39 vs 23%).

Poparcie dla wprowadzenia weryfikacji wieku w sieci przed wejściem na strony dla dorosłych





3 na 4 Polaków popiera wprowadzenie **weryfikacji wieku** w sieci dla treści dla dorosłych.

Pytanie: Czy należy wprowadzić jakąś weryfikację wieku zamiast dobrowolnych deklaracji w internecie przed wejściem na stronę z treściami pornograficznymi, alkoholami czy zakładami bukmacherskimi celem ochrony dzieci i młodzieży?

Tak
Nie mam zdania
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Anna Rywczyńska

Kierowniczka Działu Profilaktyki Cyberzagrożeń NASK

Badania przedstawione w raporcie poruszają kluczowe zagadnienia, takie jak przemoc w sieci, kontakt dzieci i młodzieży z nieodpowiednimi treściami oraz kwestia weryfikacji wieku. To, że – według wyników badania – 56% Polaków uważa, że polskie prawo nie zapewnia wystarczającej ochrony dzieci przed treściami dla dorosłych, odzwierciedla obawy o bezpieczeństwo najmłodszych w internecie. Obecne mechanizmy, bazujące na dobrowolnych deklaracjach wieku, są powszechnie uznawane za niewystarczające, co tłumaczy poparcie 73% Polaków dla rzetelniejszych narzędzi weryfikacyjnych.

Respondenci wskazują na cyfrowy certyfikat wieku, który mógłby być okazywany anonimowo, bez ujawniania danych osobowych, jako jedno z możliwych rozwiązań. Taki mechanizm mógłby skuteczniej chronić dzieci przed dostępem do nieodpowiednich treści, jednocześnie minimalizując ryzyko naruszenia prywatności. Z perspektywy legislacyjnej (DSA – Akt o Usługach Cyfrowych) może odegrać kluczową rolę w poprawie sytuacji, wymuszając na platformach większą odpowiedzialność za treści i zapewniając bezpieczne środowisko dla młodszych użytkowników.

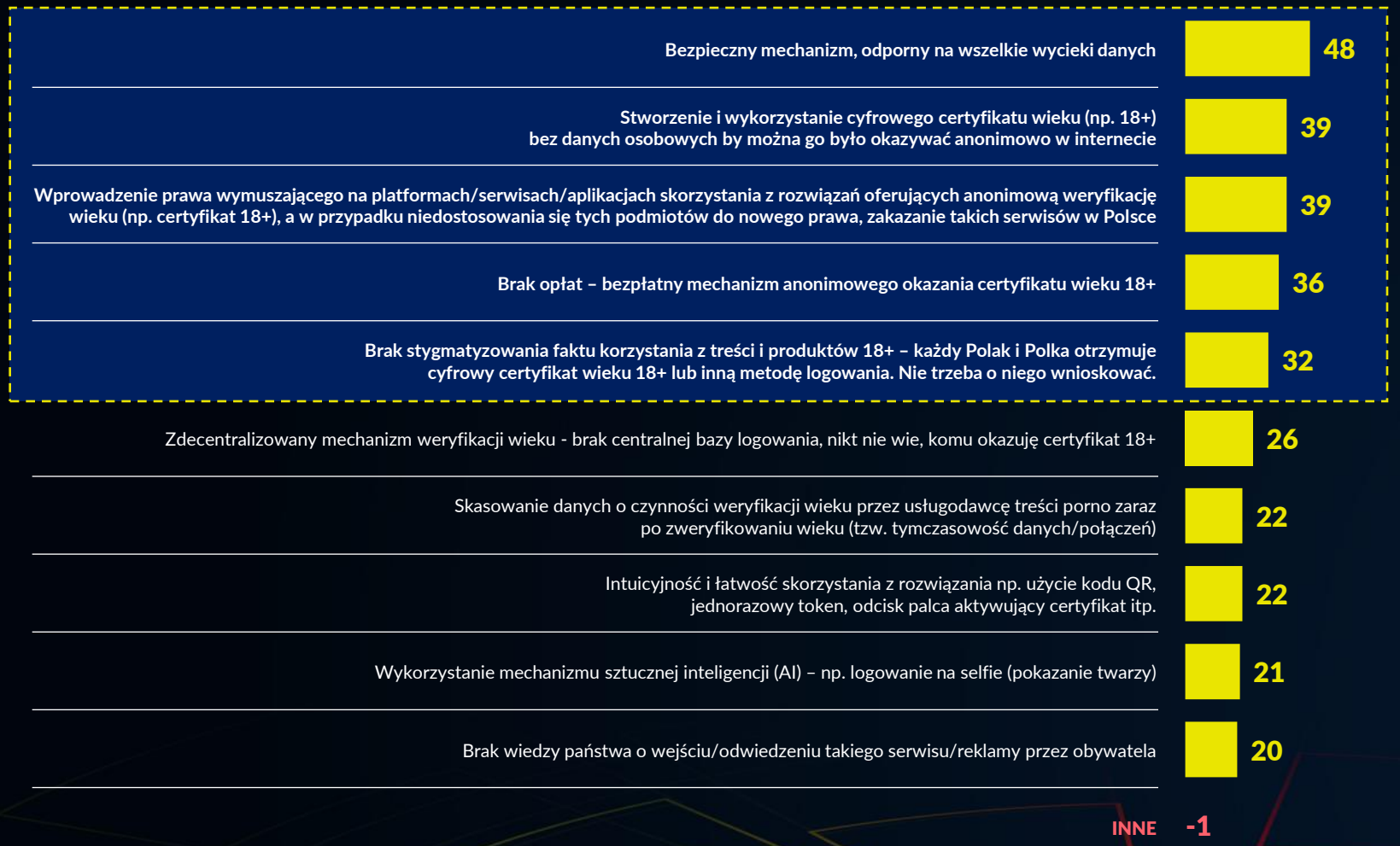
Również według badań NASK, przedstawionych w raporcie „Nastolatki wobec pornografii cyfrowej", 73% dzieci i młodzieży uważa, iż w internecie łatwo znaleźć treści o charakterze pornograficznym, a średnia wieku pierwszego kontaktu z takimi materiałami wynosi niespełna 11 lat. Dodatkowo aż 58,5% nastolatków przyznaje, że przynajmniej raz zetknęło się z materiałami pornograficznymi online, a 43% miało z nimi kontakt wielokrotnie. Te dane, zestawione z wynikami raportu „Cyberbezpieczeństwo", podkreślają pilną potrzebę skutecznej weryfikacji wieku i ochrony dzieci przed szkodliwymi treściami.

W raporcie „Cyberbezpieczeństwo" wskazano również, że połowa rodziców nie stosuje narzędzi ochrony rodzicielskiej, co mogłoby istotnie zwiększyć bezpieczeństwo młodych użytkowników. Ponadto podczas gdy 35% dorosłych przyznało, że padło ofiarą mowy nienawiści, w badaniu NASK „Nastolatki 3.0" również blisko 40% dzieci zadeklarowało, że spotkało się z wyzwiskami w sieci. Ryzyko hejtu dotyka w podobnym stopniu dziewczynki i chłopców, to dziewczynki jednak najczęściej są ofiarami przemocy na tle wyglądu fizycznego i prawie 90% z nich uważa przemoc w internecie za poważny problem. Podobnie 75% respondentów badania „Cyberbezpieczeństwo" uważa, że mowa nienawiści w sieci jest zbyt powszechna i wymaga pilnych regulacji.

Jednocześnie zjawisko przemocy cyfrowej wśród dzieci jest niedoszacowane przez rodziców – podczas gdy około 40% dzieci potwierdza, że padło ofiarą wyzywania w sieci, tylko 10% rodziców ma tego świadomość. Tymczasem dzieci, choć biegłe technologicznie, często nie są przygotowane na radzenie sobie z przemocą w sieci, a także nie zawsze dzielą się z rodzicami swoimi negatywnymi doświadczeniami. Podniesienie świadomości rodziców o zagrożeniach cyfrowych jest kluczowe, aby mogli skuteczniej wspierać swoje dzieci w bezpiecznym korzystaniu z internetu.

Ważne kwestie przy wprowadzaniu weryfikacji wieku w internecie

TOP 5



Bezpieczny, odporny na wycieki, anonimowy, bezpłatny.

To główne cechy jakie powinien spełniać mechanizm weryfikacji wieku. 4 na 10 Polaków popiera zakazanie serwisów, które nie uznałyby takiego obowiązkowego narzędzia do weryfikacji wieku.

ⓘ Pytanie wielokrotnego wyboru. Max 5 odpowiedzi.
Baza: respondenci którzy stwierdzili, że należy wprowadzić weryfikację wieku (N=735)

PŁEĆ

Mężczyźni częściej od kobiet wskazali na takie kwestie jak potrzebę braku stygmatyzowania faktu korzystania z treści i produktów 18+ (39 vs 27%), bezpieczny mechanizm, który jest odporny na wycieki danych (52 vs 45%), skasowanie danych o czynności weryfikacji wieku przez usługodawcę (26 vs 19%), intuicyjność (26 vs 19%) czy wykorzystanie AI (25 vs 19%).

Nie zaobserwowano znaczących różnic dla pozostałych odpowiedzi, a stworzenie i wykorzystanie anonimowego certyfikatu wieku poparło 41% panów vs 38% pań.

WIEK

Dal młodych osób zdecydowanie bardziej ważną kwestią niż dla osób starszych jest stworzenie i wykorzystanie cyfrowego i anonimowego certyfikatu bez danych osobowych by można go było okazywać anonimowo w internecie (49 vs 33%). Podobnie ważną kwestią jest brak stygmatyzowania (40 vs 28%) czy brak wiedzy państwa o wejściu na treści 18+ (22 vs 13%).

Osoby starsze częściej wskazały na potrzebę stworzenia bezpiecznego mechanizmu odpornego na wycieki danych (53 vs 42%) czy zdecentralizowanego mechanizmu weryfikacji wieku (34 vs 27%).

MIEJSCE ZAMIESZKANIA

Mieszkańcy dużych miast trochę częściej wskazali na potrzebę bezpiecznego mechanizmu odpornego na wycieki danych (57 vs 50%).

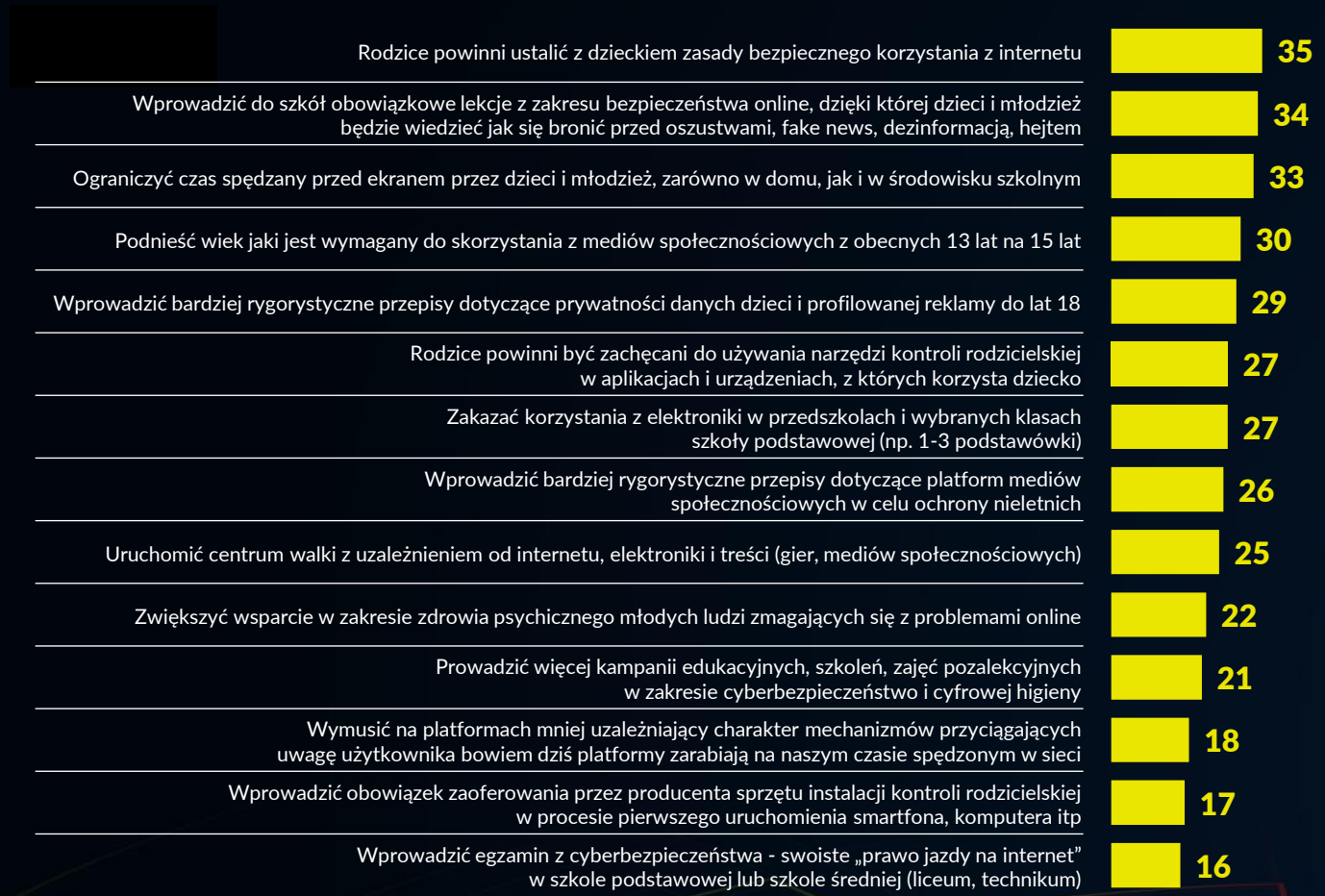
Osoby mieszkające na wsi częściej wskazały na potrzebę braku stygma0tyzowania z faktu korzystania z treści i produktów 18+ (34 vs 27%) czy stworzenie i wykorzystanie cyfrowego certyfikatu wieku (41 vs 35%).

WYKSZTAŁCENIE

Dla osób z wyższym wykształceniem bardziej niż dla osób z wykształceniem podstawowym ważniejsza jest kwestia skasowania danych o czynności weryfikacji wieku (25 vs 17%) i brak stygmatyzowania (34 vs 28%).

Osoby z wykształceniem podstawowym częściej wskazały na potrzebę zapewnienia intuicyjności (30 vs 19%), stworzenie zdecentralizowanego mechanizmu weryfikacji wieku (31 vs 23%) czy brak wiedzy państwa o fakcie korzystania z produktów i usług 18+ (25 vs 19%).

Co jeszcze dodatkowo można zrobić, aby podnieść bezpieczeństwo dzieci i nastolatków w sieci?



1 na 3 Polaków popiera ograniczenie czasu przed ekranem, lekcje z cyberbezpieczeństwa w szkole czy ustalenie przez rodziców zasad dla dzieci korzystania z internetu.

27% popiera zakazanie korzystania z elektroniki w przedszkolach i wybranych klasach szkoły podstawowej.

ⓘ Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni częściej od kobiet wskazali na potrzebę wprowadzenia do szkół obowiązkowych lekcji z zakresu cyberbezpieczeństwa (37 vs 31%) czy potrzebę wprowadzenia bardziej rygorystycznych przepisów dotyczących prywatności dzieci i profilowanej reklamy poniżej 18 roku życia (32 vs 27%).

Kobiet częściej wskazały na odpowiedź, że to rodzice powinni ustalić z dzieckiem zasady bezpiecznego korzystania z internetu (40 vs 31%). Kobiety częściej też wskazały na konieczność ograniczenia czasu spędzanego przed ekranem (36 vs 29%)

WIEK

Osoby młodsze częściej od osób starszych wskazały na potrzebę wprowadzenia swoistego prawa jazdy na internet (24 vs 8%) czy wymuszenie na platformach stosowania mniej uzależniających algorytmów (26 vs 12%). Młode osoby częściej od osób starszych popierają wprowadzenie zakazu korzystania z elektroniki w przedszkolach i wybranych klasach szkoły podstawowej (33 vs 24%).

Osoby starsze częściej wskazały by to rodzice ustalali z dzieckiem zasady bezpiecznego korzystania z internetu (42 vs 33%), by wprowadzono obowiązek zaoferowania przez dostawcę sprzętu obowiązkowej instalacji kontroli rodzicielskiej (17 vs 10%) oraz częściej wskazały na potrzebę ograniczenia czasu przed ekranem (37 vs 30%).

MIEJSCE ZAMIESZKANIA

Nie zaobserwowano znaczących różnic w odpowiedziach z uwagi na miejsce zamieszkania respondenta. Jedyne różnice można zaobserwować w trzech odpowiedziach dotyczących uruchomienia centrum walki z uzależnieniem od internetu, elektroniki (30 vs 24% – działanie to bardziej preferują osoby dużych miast).

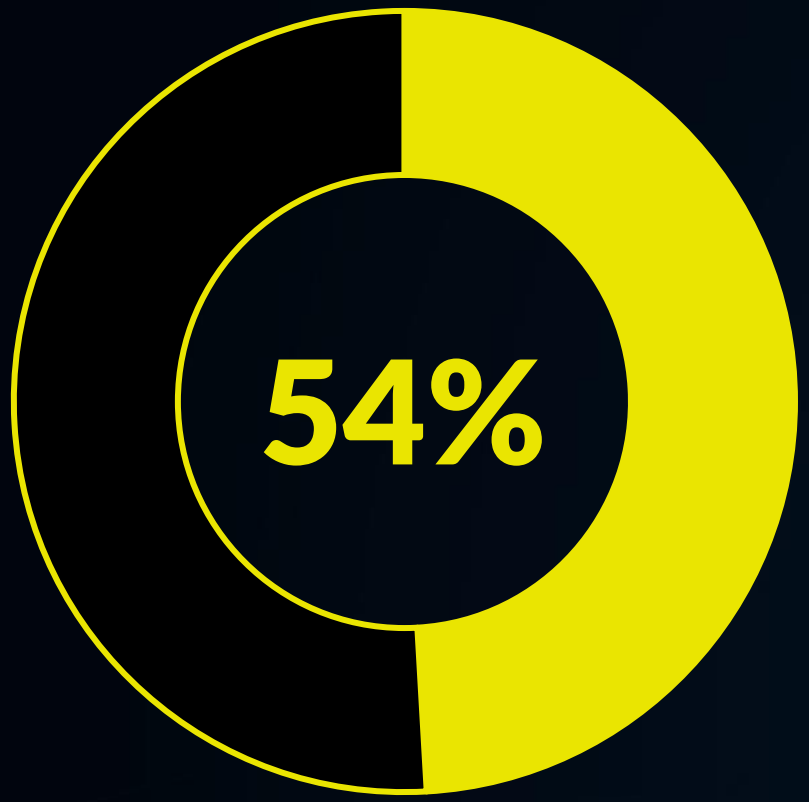
Z kolei osoby mieszkające na wsi trochę bardziej preferują podwyższenie minimalnego wieku jaki uprawnia do skorzystania z mediów społecznościowych (33 vs 28%) czy wprowadzenie bardziej rygorystycznych przepisów w zakresie prywatności dzieci i profilowania reklamy do lat 18+ (30 vs 24%).

WYKSZTAŁCENIE

Największe różnice w odpowiedziach można zaobserwować z punktu widzenia posiadanego wykształcenia. Osoby z wyższym wykształceniem zdecydowanie częściej wskazują na potrzebę wprowadzenia obowiązkowych lekcji o cyberbezpieczeństwie do szkół (42 vs 24%), postulują zwiększenie wymaganego wieku jaki uprawnia do skorzystania z mediów społecznościowych (36 vs 19%) czy wprowadzenia swoistego prawa jazdy na korzystanie z internetu (19 vs 9%).

Osoby z wykształceniem podstawowym częściej wskazały na jedną odpowiedź – uruchomienie centrum walki z uzależnieniem od internetu i elektroniki (34 vs 25%).

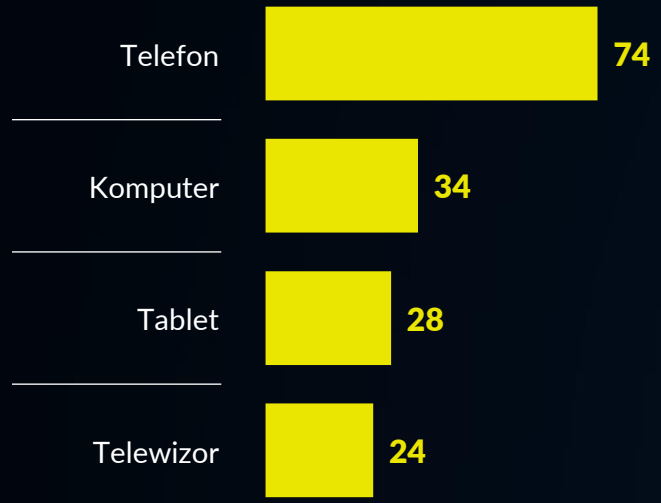
Czy Polacy stosują kontrolę rodzicielską na urządzeniach elektronicznych?



Co drugi rodzic posiadający dziecko poniżej 18 roku życia deklaruje stosowanie kontroli rodzicielskiej na urządzeniach elektronicznych.

Pytanie jednokrotnego wyboru
Baza: osoby posiadające dzieci poniżej 18 roku życia (N=296)

Na jakich urządzeniach stosowana jest kontrola rodzicielska?



4 na 5 rodziców wykorzystujących kontrolę rodzicielską stosuje ją na smartfonie, a następnie komputerze (34%).

Pytanie wielokrotne wyboru
Baza: osoby posiadające dzieci poniżej 18 roku życia oraz które zadeklarowały korzystanie z kontroli rodzicielskiej (N=159)

Katarzyna Nowicka

Rzecznik prasowy Stowarzyszenia Twoja Sprawa, prowadzi portal opornografii.pl oraz szkolenia dla rodziców i pedagogów „Jak chronić dziecko przed pornografią?”

Jako organizacja, która od kilkunastu lat zajmuje się ochroną dzieci przed pornografią, zwracamy szczególną uwagę na rozdział raportu „Ochrona dzieci i młodzieży w internecie”. Zawarte w nim dane pokazują bowiem, jak dorośli postrzegają tę kwestię i jakie rozwiązanie należy ich zdaniem wprowadzić, aby ochronę dzieci zwiększyć.

Aż 56 proc. badanych uznało, że polskie prawo ze względu na nierzetelne sprawdzanie pełnoletności nie chroni odpowiednio dzieci przed takimi treściami jak m.in. pornografia. 20% uważa inaczej, a 24% nie ma zdania w tej sprawie.

Choć te 56% to całkiem sporo, wynik ten pokazuje też, jak ważne jest podnoszenie świadomości dorosłych. Jeśli bowiem chodzi o pornografię, to dzieci w internecie nie są przed nią chronione w żaden sposób. Trudno za ochronę uznać przecież kliknięcie, że ma się 18 lat... Trwa to zaledwie kilka sekund i umożliwia wejście w świat wulgarny, brutalny i uprzedmiatawiający drugiego człowieka, w świat treści, które wpływają negatywnie na psychikę dzieci i na ich przyszłość.

Na uwagę zasługuje też fakt, że większa jest świadomość osób w najmłodszych grupach wiekowych 18–29 i 30–39 lat. One częściej wskazują na niewystarczającą ochronę dzieci.

Do optymistycznych akcentów należy niewątpliwie zgoda dorosłych, że to, co funkcjonuje w świecie rzeczywistym, czyli na przykład zakaz sprzedaży alkoholu, energetyków czy treści pornograficznych dzieciom w sklepie, powinno być zabronione i przestrzegane również w internecie. W tym przypadku „tak” mówi już aż 75% uczestników badania.

Co bardzo ważne, niewiele mniej, bo 73% ankietowanych wyraża poparcie dla wprowadzenia weryfikacji wieku w internecie przed wejściem na strony dla dorosłych. Najważniejszą wskazywaną kwestią jest to, żeby był to mechanizm odporny na wszelkie wycieki danych.

Jeśli chodzi o pozostałe działania zwiększające ochronę dzieci, wymieniane są m.in. zasady bezpiecznego korzystania z internetu, wprowadzenie lekcji z zakresu bezpieczeństwa online, ograniczenie czasu spędzanego przed ekranem zarówno w domu jak i w szkole. Wiele tych kwestii poruszamy na naszych szkoleniach dla rodziców i pedagogów „Jak chronić dziecko przed pornografią?”. Cieszy nas, że świadomość w tym zakresie rośnie.

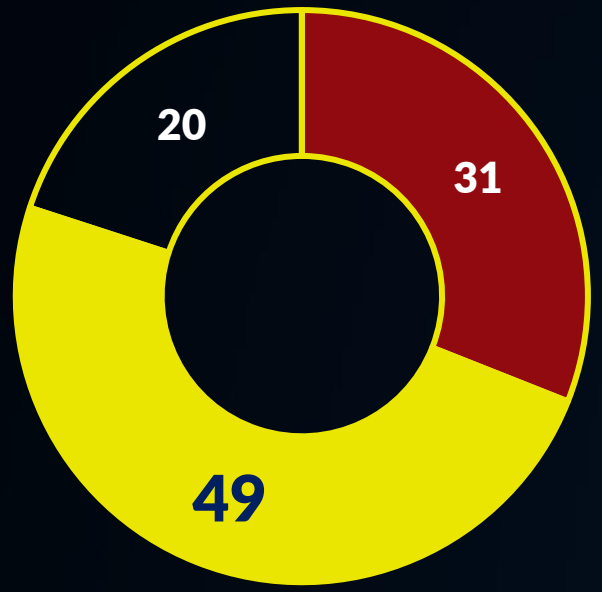
Podsumowując. Z raportu jasno wynika, że większość dorosłych uważa, że dzieci nie są odpowiednio chronione przez polskie prawo przed dostępem do takich treści jak chociażby pornografia. Jeszcze więcej osób jest za tym, żeby te same zasady obowiązywały w świecie realnym i w sieci. I wreszcie większość popiera wprowadzenie weryfikacji wieku w internecie, tak aby dostęp do pewnych treści miały tylko osoby pełnoletnie. Byłoby to rozwiązanie w dużej mierze skuteczne, a nie tak jak teraz – fikcyjne.

Mamy nadzieję, że wyniki tego raportu, jak i innych wcześniejszych badań wskazujących na skalę kontaktu dzieci z pornografią, dadzą do myślenia decydentom, dla których dobro dzieci i ich przyszłość powinny być absolutnym priorytetem.

2.8.

Czy ważny jest dla nas kraj pochodzenia dostawcy rozwiązań z zakresu cyberbezpieczeństwa?

Czy ważny jest kraj pochodzenia dostawców rozwiązań z zakresu cyberbezpieczeństwa?



Połowa Polaków deklaruje, że przy kupnie lub korzystaniu z rozwiązań z zakresu cyberbezpieczeństwa ważny jest kraj pochodzenia dostawcy (np. antywirusa).

Aż co trzeci nie ma zdania w tej kwestii.

Tak
Nie mam zdania
Nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Jakie kraje są preferowane przez konsumentów?

TOP 3

7* na 10 badanych dla których kwestia kraju pochodzenia jest ważna preferuje dostawców z Polski.

Polska, kraje anglosaskie i Unia Europejska to preferowane kierunki pochodzenia dostawców rozwiązań i usług z zakresu cyberbezpieczeństwa. Izrael czy Korea Południowa cieszą się podobnym zaufaniem jak Chiny, Indie czy Rosja.

* 33,5% z wszystkich Polaków preferuje Polskę

Pytanie wielokrotnego wyboru
Baza: respondenci którzy odpowiedzieli TAK (N=486)

gen. bryg. rez. Włodzimierz Nowak

Były pełnomocnik Ministra Cyfryzacji ds. cyberbezpieczeństwa, obecnie niezależny ekspert cyberbezpieczeństwa z doświadczeniem biznesowym, militarnym i administracji państwowe

Badanie jasno pokazuje stanowisko i preferencje naszego społeczeństwa odnośnie do pochodzenia produktów lub usług, 49% ankietowanych wskazuje na bezpośrednią zależność bezpieczeństwa od kraju pochodzenia. Świadczy to o pewnej dojrzałości społeczeństwa, które potrafi połączyć sytuację geopolityczną (sojusze, konflikty) z praktycznym wpływem na nasze bezpośrednie bezpieczeństwo w cyberprzestrzeni. O wysokim poziomie świadomości świadczy również wskazanie Polski jako najbardziej pożądanego dostawcy produktów i usług. Daje to podstawy do rozwoju rodzimych przedsiębiorstw i akceptację społeczeństwa dla działań rządu zmierzających w tym kierunku. W Top 3 wskazano również wysoki poziom akceptacji (43%) dla produktów i usług pochodzących z USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii. O ile akceptacja produktów i usług z USA i Wielkiej Brytanii jest w pełni zrozumiała ze względu na wysoki poziom zaawansowania technologicznego i bliskie partnerstwo polityczne, ekonomiczne i wojskowe, o tyle wskazanie Australii i Nowej Zelandii nie ma podstaw wynikających z doświadczeń bieżącej współpracy. Widać w tym przypadku brak refleksji i realistycznej oceny możliwości współpracy, szczególnie w czasie potencjalnego konfliktu, gdy łańcuchy dostaw zostają poddane próbie odporności na zakłócenia.

W obszarze Top 3 znalazły się również kraje Unii Europejskiej (39%), co jest zrozumiałe i logiczne. Współpraca w ramach UE jest elementem wzmacniającym poziom cyberbezpieczeństwa wszystkich krajów.

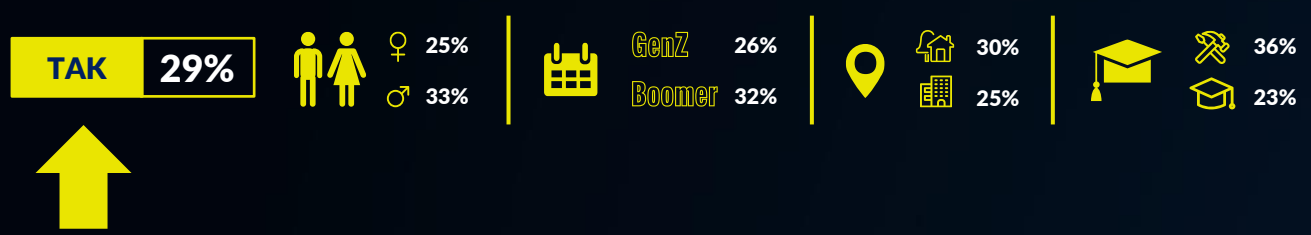
W badaniu 49% respondentów wskazało, że kraj pochodzenia produktów lub usług jest istotny z punktu widzenia bezpieczeństwa. Statystycznie zdecydowanie więcej mężczyzn niż kobiet tak uważa (52 do 45), z kolei zdecydowanie więcej kobiet niż mężczyzn nie ma zdania na ten temat (37 do 25). Większy odsetek kobiet niemających zdania może być efektem mniejszego zainteresowania technologiami ze strony kobiet lub mniejszą pewnością oceny bieżących problemów wynikających z postępu technologicznego. Badanie pokazuje również, że wiek respondentów, a tak naprawdę ich doświadczenie zawodowe, ma wpływ na ich opinię. W grupie wiekowej 18–29 lat aż 34% odpowiedziało, że kraj pochodzenia nie ma wpływu na bezpieczeństwo, podczas gdy w grupie wiekowej 50–59 lat, czyli tej najbardziej doświadczonej, było to 16%. Takie wyniki mogą wskazywać na niewystarczający transfer wiedzy od osób bardziej doświadczonych do rozpoczynających karierę zawodową. Badanie pokazuje wyraźnie, że miejsce zamieszkania i wielkość miejscowości nie ma istotnego wpływu na opinię przedstawioną w ankiecie. Z kolei w odniesieniu do wykształcenia respondentów można zauważyć pewną prawidłowość: ci z wykształceniem podstawowym i zasadniczym zawodowym preferują produkty Polskie i dostarczane przez kraje UE, na trzecim miejscu pochodzące z USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii, co wskazuje na preferencje współpracy europejskiej i stawiania na rozwój współpracy w ramach UE. Respondenci z wykształceniem średnim i wyższym preferują natomiast Polskie produkty, następnie te pochodzące z USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii, a na trzecim miejscu z krajów UE. Ogólnie rzecz ujmując, oba podejścia są słuszne i mają swoje uzasadnienie. Osoby z wyższym i średnim wykształceniem zwracają większą uwagę na jakość technologii, a osoby z wykształceniem średnim i podstawowym uznały za ważne dostępność technologii i jej rozwój w ramach EU.

Warto również zauważyć, że niewielki odsetek ankietowanych wykazał preferencje dla produktów i usług pochodzących z Chin pomimo dużego nasycenia rynku i infrastruktury telekomunikacyjnej w Polsce produktami pochodzącymi z tego kraju. Wskazuje to na wzrost świadomości związany z zapewnieniem bezpiecznych łańcuchów dostaw i często pojawiającej się dyskusji na temat dostawców wysokiego ryzyka. Nie przekłada się to jednak na praktyczne zachowanie społeczeństwa, co widać po utrzymującej się na wysokim poziomie sprzedaży produktów pochodzenia chińskiego.

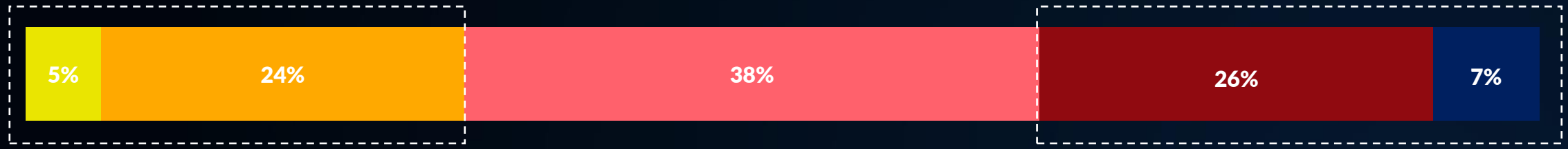
2.9.

Jak cyberbezpieczny jest nasz kraj?

Czy polskie państwo traktuje priorytetowo kwestię cyberbezpieczeństwa i podejmuje stosowne działania



Polacy są podzieleni w sprawie oceny działań państwa polskiego



Zdecydowanie tak
Raczej tak
Nie wiem / nie mam zdania
Raczej nie
Zdecydowanie nie

Pytanie jednokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

Przyczyny incydentów naruszających cyberbezpieczeństwo w administracji, urzędach i firmach

TOP 5

Wśród dwóch z pięciu najpopularniejszych powodów incydentów w organizacjach w Polsce występuje **czynnik ludzki** - brak wiedzy wśród ludzi (28%) oraz niestosowanie się pracowników do polityk cyberbezpieczeństwa (24%). Równie ważnym powodem jest indywidualne **działanie hackerów** jak i profesjonalnych grup, w tym sponsorowanych przez **obce służby.**

Na **brak środków** wskazało jedynie **16% badanych.**

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

gen. bryg. rez. Włodzimierz Nowak

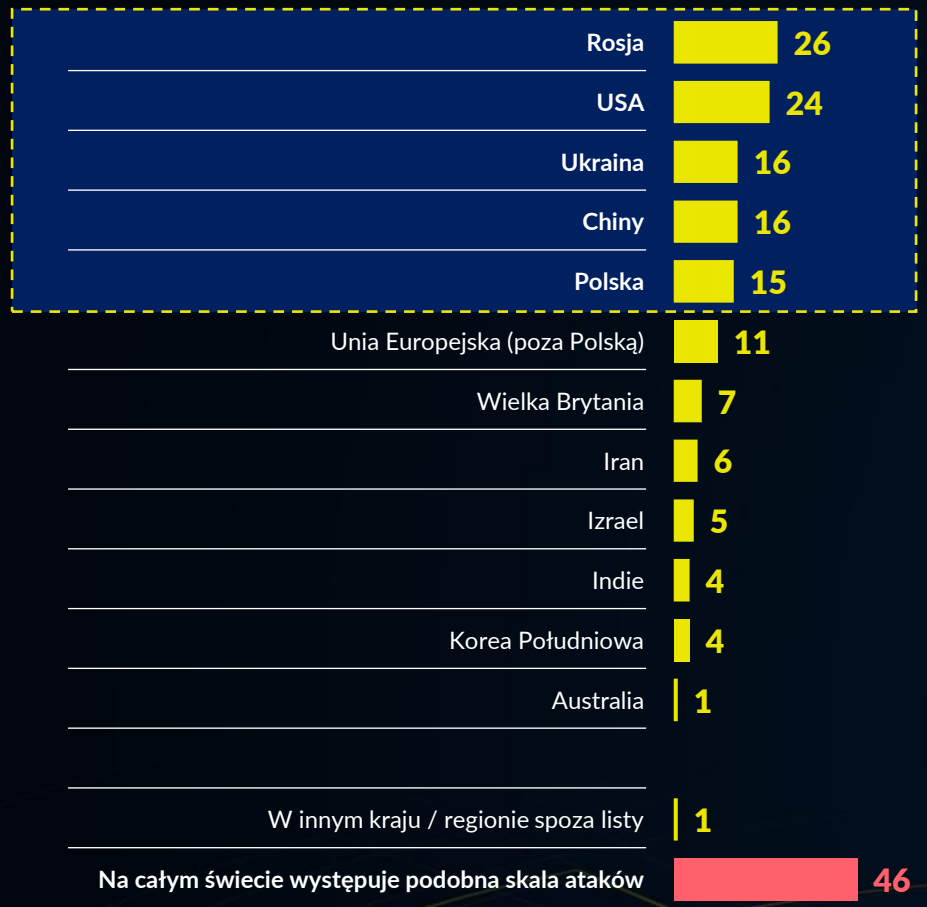
Były pełnomocnik Ministra Cyfryzacji ds. cyberbezpieczeństwa, obecnie niezależny ekspert cyberbezpieczeństwa z doświadczeniem biznesowym, militarnym i administracji państwowe

Stopień zagrożenia cyberatakami w poszczególnych krajach

Top5 wskazujący w których krajach społeczeństwo i organizacje są najbardziej narażone na cyberataki pokazuje, jak bardzo nasze społeczeństwo jest niedoinformowane i błędnie ocenia sytuację międzynarodowego cyberbezpieczeństwa. Dotyczy to zarówno oceny kobiet jak i mężczyzn. Wskazanie Rosji jako kraju najbardziej narażonego na cyberataki to jaskrawy przejaw niewiedzy. Rosja wprowadziła znaczący poziom separacji zasobów sieciowych, budując narodowy intranet, zabezpieczony przed dostępem informacji z krajów demokratycznych i ograniczający obywatelom swobodny dostęp do wymiany informacji z krajami obozu demokratycznego, jednocześnie rozbudowując rządowe komórki aktywnych działań w cyberprzestrzeni z zadaniami szerzenia dezinformacji i sabotażu cyfrowego w krajach demokratycznych. Tak więc Rosja nie jest ofiarą ataków cyfrowych, a jednym z największych ośrodków odpowiedzialnych za ataki cyfrowe na kraje demokratyczne. W Top5 na piątym miejscu znalazła się również Polska, zarówno jednak kobiety, jak i mężczyźni ocenili, że Polska jest dużo mniej zagrożona cyberatakami niż Rosja. Ocena respondentów jest podobna we wszystkich grupach wiekowych, nie zależy od wielkości miejscowości i wykształcenia. Widać więc, że polityka informacyjna o źródłach i skali ataków jest niewystarczająca, ataki na Polskę ze strony Rosji są na wysokim poziomie intensywności, więc należy o tym informować społeczeństwo, by kształtować właściwe postrzeganie sytuacji w cyberprzestrzeni. Potwierdzeniem tego jest również niedoszacowanie ataków na Ukrainę, Izrael czy Koreę Południową. Jednocześnie ankietowani w ponad 34–59% przypadków wskazali, że podobna skala ataków występuje na całym świecie, nie biorąc pod uwagę skali informatyzacji i roli kraju w światowym systemie polityczno-gospodarczo-militarnym.

W których krajach społeczeństwo i organizacje są najbardziej narażone na cyber ataki?

TOP 5



Rosja i Stany Zjednoczone to dwa kraje, w których według Polaków ma dochodzić do **największej skali cyberataków.**

Na Polskę wskazało **15% badanych,** podobny odsetek co na Ukrainę czy Chiny. Jedynie ok. 5% badanych wskazało na Iran lub Izrael.

Należy jednak zaznaczyć że zdaniem aż **46%** respondentów **na całym świecie występuje podobna skala** ataków - niezależnie od kraju czy regionu.

Pytanie wielokrotnego wyboru
Baza: wszyscy respondenci w badaniu (N=1000)

PŁEĆ

Mężczyźni częściej niż kobiety wskazali, że stopień zagrożenia cyberatakami czy incydentami jest większy w Rosji (30 vs 22%), w Polsce (19 vs 11%) czy USA (26 vs 21%).

Z kolei kobiety zdecydowanie częściej wskazały, że na całym świecie występuje podobna skala ataków (53 vs 39%).

WIEK

Największe różnice w odpowiedziach można zaobserwować z punktu widzenia wieku respondenta.

Osoby starsze zdecydowanie częściej wskazały niż osoby młodsze, że na całym świecie występuje podobna skala cyberataków (59 vs 34%). Podobnie częściej wskazano na Unię Europejską jako częstszy cel ataków (15 vs 9%).

Osoby młodsze częściej wskazały, że skala ataków jest większa w Ukrainie (22 vs 10%), Iranie (12 vs 3%), USA (25 vs 17%) czy w Polsce (17 vs 9%).

MIEJSCE ZAMIESZKANIA

Osoby z dużych miejscowości częściej wskazywały na większa skalę cyberataków w Chinach (25 vs 13%), w USA (35 vs 23%) czy na terenie UE z wyłączeniem Polski (15 vs 10%).

Osoby mieszkające na wsi częściej wskazały, że skala cyberataków jest podobna na całym świecie (47 vs 38%) czy jest wyższa w Korei Południowej (6 vs 2%).

WYKSZTAŁCENIE

Osoby z wyższym wykształceniem częściej wskazały na odpowiedź, że skala ataków jest wyższa w Rosji (30 vs 15%), w USA (29 vs 19%), w Ukrainie (24 vs 14%) czy w Polsce (17 vs 9%).

Osoby z wykształceniem podstawowym częściej wskazały, że skala cyber ataków jest podobna na całym świecie (50 vs 40%).

gen. bryg. rez. Włodzimierz Nowak

Były pełnomocnik Ministra Cyfryzacji ds. cyberbezpieczeństwa, obecnie niezależny ekspert cyberbezpieczeństwa z doświadczeniem biznesowym, militarnym i administracji państwowe

Przyczyny incydentów naruszających cyberbezpieczeństwo administracji

Ocena najczęstszych przyczyn incydentów naruszających cyberbezpieczeństwo administracji (centralnej, samorządowej itp.) w urzędach lub firmach w Polsce nie zależy w znaczącym stopniu od płci, wieku, wykształcenia ani wielkości miejscowości. Wśród zauważanych przyczyn incydentów brak jest zdecydowanego faworyta. Upatruje się ich zarówno w braku świadomości czy wiedzy, jak i działań indywidualnych hakerów, zorganizowanych grup hakerskich, zaniedbań pracowników, luk w oprogramowaniu, zaniedbań personelu IT czy celowo stworzonych „tylnych drzwi" w sprzęcie i oprogramowaniu pochodzącym spoza UE. Na uwagę zasługuje tu ocena respondentów w przedziale wiekowym 60–75 lat, którzy wskazują jako główną przyczynę powstawania incydentów ataki indywidualnych hakerów (36%). Podobne zdanie maja respondenci z podstawowym wykształceniem (32%). Z kolei grupa wiekowa 50–59 lat w większości (31%) uważa, że to działania szpiegowskie i zorganizowane grupy azerskie są główną przyczyną niepożądanych incydentów (31%). Ankietowani posiadający wyższe wykształcenie uważają, że przyczyną incydentów jest niestosowanie się pracowników do polityk cyberbezpieczeństwa. Mniejsza, choć znacząca liczba ankietowanych jako przyczynę incydentów wskazuje brak odpowiednich działań ze strony kierownictwa instytucji, brak odpowiednich środków ochrony (sprzętu, oprogramowania), podatność użytkowników na manipulacje (tu głównie respondenci z grupy wiekowej 18–29 lat – 25% i z grupy posiadającej podstawowe wykształcenie – 27%) oraz brak kontroli ze strony firm, urzędów czy państwa.

Ocena państwa polskiego w kwestii cyberbezpieczeństwa

Ocena, czy polskie państwo traktuje priorytetowo kwestie związane z cyberbezpieczeństwem i podejmuje stosowne działania, wskazuje przewagę osób oceniających ten proces jako niewystarczający (zdecydowanie nie i raczej nie odpowiedziało 33% badanych). Mniej respondentów oceniło te działania pozytywnie (raczej tak i zdecydowanie tak odpowiedziało 29%). Zdecydowana większość (38%) nie ma zdania na ten temat, co może świadczyć o niewystarczającej liczbie informacji o działaniach podejmowanych przez państwo. Pomimo zdecydowanej promocji bezpieczeństwa w sieci przez Ministerstwo Cyfryzacji na portalach specjalistycznych i w mediach społecznościowych przekaz ten nie dociera do większości społeczeństwa. Potwierdza to fakt niewielkiej liczby ocen „zdecydowanie tak", mieszczących się w przedziale od 2 do 8% i „zdecydowanie nie", gdzie przedział ten wynosi 4–10%. Brak wyrazistych i skutecznych (odczuwalnych przez społeczeństwo) działań państwa, spowodował, że większość głosów rozkłada się na oceny: raczej tak – 16–29%, raczej nie – 18–35% – oraz nie mam zdania – 27–45%. Brak zdania deklaruje 45% osób z wykształceniem zawodowym, 44% osób mieszkających w miejscowości 50–500 tys. mieszkańców oraz 44% osób w wieku 50–59 lat. Tak niezadowalające rezultaty mogą być skutkiem wielu czynników. Jednym z nich może być zbyt specjalistyczny przekaz medialny, który jest niezrozumiały dla większości społeczeństwa. Kolejnym – niespełnione oczekiwania społeczeństwa związane ze zmianą władzy. Oczekiwano zdecydowanego zwrotu w obszarze cyberbezpieczeństwa, a mamy kontynuację działań poprzedniego rządu firmowaną przez nowe kierownictwo Ministerstwa Cyfryzacji. Kolejną przyczyną może być zbytnie eksponowanie zagrożeń w przekazach medialnych, co sprawia wrażenie oblężonej twierdzy powodując niepokój i nie budując zaufania do działań państwa.

Radosław Nożykowski

Adwokat, Baker McKenzie Krzyżowski i Wspólnicy sp.k.

Z uwagi na rosnące znaczenie cyberbezpieczeństwa dla nowoczesnej gospodarki, Unia Europejska zdecydowała się zwiększyć bezpieczeństwo informatyczne wszystkich kluczowych sektorów gospodarki.
Do głównych aktów związanych ze strategią budowy nowego systemu cyberbepieczeństwa w Unii Europejskiej należy zaliczyć:

A. Rozporządzenie DORA (sektor finansowy),

B. Dyrektywa NIS-2 (sektory pozafinansowe),

C. Cyber Resilience Act (produkty z tzw. elementem cyfrowy),

oraz towarzyszące im krajowe przepisy implementujące o krajowym systemie cyberbezpieczeństwa (w przypadku Polski – nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa).

A. Rozporządzenie DORA uchwalono 14.12.2022r. i weszło w życie 16.1.2023 r. Podmioty objęte rozporządzeniem będą miały obowiązek stosowania przepisów od 17.1.2025 r.

Rozporządzenie DORA ustanawia wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych firm i instytucji działających w sektorze finansowym, a także kluczowych zewnętrznych dostawców usług związanych z ICT (technologiami informacyjno-komunikacyjnymi), takich jak platformy w chmurze czy usługi analizy danych. Rozporządzenie ujednolica także inne segmenty odnoszące się do zarządzania ryzykiem związanym z ICT, które zakresem swego oddziaływania obejmują kilka innych rozporządzeń i dyrektyw z unijnego pakietu finansowego.

B. Dyrektywa NIS-2 została uchwalona 14.12.2022 r., a Państwa członkowskie będą zobowiązane do stosowania jej przepisów od dnia 18.10.2024 r., a więc na kilka miesięcy przed rozpoczęciem biegu obowiązywania przepisów Rozporządzenia DORA.

Dyrektywa NIS 2 zmienia ramy systemu cyberbezpieczeństwa w Unii Europejskiej wprowadzając m.in. nowe obowiązki dla państw członkowskich, nowy zakres podmiotów objętych obowiązkami wynikającymi z cyberbezpieczeństwa oraz kompetencje organów UE w związku z nadzorem wykonywania tych obowiązków. Polski projekt nowelizacji KSC ma służyć implementacji przepisów dyrektywy. W związku z tym, rozszerzeniu ulegnie krąg podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa.

C. Cyber Resilience Act jako trzeci wśród triady nadchodzących zmian w systemie cyberbezpieczeństwa w UE nie został jeszcze uchwalony. Projekt przewiduje jednak jego wejście w życie tego rozporządzenia w drugiej połowie 2024 r. (z uwagi na opóźnienie w jego uchwaleniu przesunięciu ulegnie najpewniej także data jego wejścia w życie). Przez okres 3 lat od dnia wejścia w życie CRA, zobowiązane podmioty będą miały czas na wprowadzanie na unijny rynek produktów zgodnych z jego przepisami.

CRA swoją uwagę skupia przede wszystkim na ochronie konsumentów oraz firm kupujących lub korzystających z produktów lub oprogramowania z komponentem cyfrowym. Rozporządzenie zakłada, że nieodpowiednie zabezpieczenia staną się przeszłością dzięki wprowadzeniu obowiązkowych wymogów w zakresie cyberbezpieczeństwa dla producentów i importerów/dystrybutorów takich produktów, przy czym ochrona ta obejmie cały cykl życia produktu.

Etapy budowy systemu cyberbezpieczeństwa

Akty prawne	Uchwalono	Data wejścia w życie / termin implementacji	Implementacja – nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa
Rozporządzenie DORA (sektor finansowy)	14.12.2022 r.	17.01.2025 r. (działanie bezpośrednie)	Regulacja uzupełniająca DORA: na etapie prac legislacyjnych – planowana data wejścia w życie: 17.01.2025 r.
Dyrektywa NIS-2	14.12.2022 r.	17.10.2024 r. (termin na implementację)	Implementacja NIS 2 do polskiego prawa: na etapie prac legislacyjnych. Planowana data wejścia w życie: po upływie miesiąca od dnia ogłoszenia ustawy.
Cyber Resilience Act (rozporządzenie)	W toku prac legislacyjnych w UE		

Rozporządzenie DORA

w sprawie operacyjnej odporności cyfrowej sektora finansowego

Kamień milowy nad bezpieczeństwem sektora finansowego oraz rynku

- Rozporządzenie DORA ustanawia wymogi dotyczące **bezpieczeństwa sieci i systemów informatycznych** firm i instytucji działających w sektorze finansowym, a także kluczowych zewnętrznych dostawców usług związanych z ICT (technologiami informacyjno-komunikacyjnymi), takich jak platformy w chmurze czy usługi analizy danych. Wymogi te są jednolite we wszystkich państwach członkowskich UE.
- Rozporządzenie ujednolica także inne segmenty odnoszące się do zarządzania ryzykiem związanym z ICT, które zakresem swego oddziaływania obejmują kilka innych rozporządzeń i dyrektyw z unijnego pakietu finansowego.
- Rozporządzenie DORA uchwalono 14.12.2022r. i weszło w życie 16.1.2023 r. Podmioty objęte rozporządzeniem będą miały obowiązek stosowania przepisów **od 17.1.2025 r.**

Materiał powstał przy wsparciu Baker McKenzie.

Dyrektywa NIS-2

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii

- Poza wprowadzeniem nowego systemu regulacji i obowiązków nakładanych na podmioty finansowe przez Rozporządzenie DORA, istotne zmiany w systemie cyberbezpieczeństwa w Unii Europejskiej zaszły także wraz z uchwaleniem Dyrektywy NIS 2.

- Jest to znacząca zmiana ram systemu cyberbezpieczeństwa w Unii Europejskiej, wprowadzając m.in. obowiązki dla państw członkowskich, nowy zakres podmiotów objętych obowiązkami wynikającymi z cyberbezpieczeństwa oraz kompetencje organów UE w związku z nadzorem wykonywania tych obowiązków.

- Zgodnie z dyrektywą, państwa członkowskie powinny wdrożyć nowe przepisy do 17.10.2024 r. Polski projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC) ma służyć implementacji przepisów dyrektywy. W związku z tym, rozszerzeniu ulegnie krąg podmiotów objętych przepisami ustawy o KSC. Zgodnie z nowym podziałem, nowelizacja przewiduje wprowadzenie nowych obowiązków na podmioty kluczowe i podmioty ważne (uwaga: nowelizacja KSC zakłada istotne zmiany w zakresie w porównaniu do NIS 2. Nowelizacja zakłada również stosowanie mechanizmów, takich jak 5G Toolbox, do ustalenia dostawców wysokie ryzyka (HRV) również w innych sektorach niż tylko sektor łączności.

Dyrektywa NIS-2

Sektory kluczowe i ważne

Sektory kluczowe

- Energetyka
- Transport
- Bankowość
- Infrastruktura rynków finansowych
- Opieka zdrowotna
- Woda pitna
- Ścieki
- Infrastruktura cyfrowa
- Zarządzanie usługami ICT (między przedsiębiorstwami)
- Podmioty administracji publicznej

Sektory ważne

- Usługi pocztowe i kurierskie,
- Gospodarowanie odpadami
- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, przetwarzanie i dystrybucja żywności
- Produkcja
- Dostawcy usług cyfrowych
- Badania naukowe

CRA – Cyber Resilience Act

- **Cyber Resilience Act (CRA)** ma na celu ochronę konsumentów i firm kupujących lub korzystających z produktów lub oprogramowania z komponentem cyfrowym. Rozporządzenie zakłada, że nieodpowiednie zabezpieczenia staną się przeszłością dzięki wprowadzeniu obowiązkowych wymogów w zakresie cyberbezpieczeństwa dla producentów i importerów/dystrybutorów takich produktów, przy czym ochrona ta obejmie cały cykl życia produktu.
- Rozporządzenie o odporności cybernetycznej ma na celu zagwarantować:
  - zharmonizowane zasady przy wprowadzaniu na rynek produktów lub oprogramowania z komponentem cyfrowym;
  - ramy wymogów cyberbezpieczeństwa regulujące planowanie, projektowanie, rozwój i utrzymanie takich produktów, z obowiązkami, które należy spełnić na każdym etapie łańcucha wartości;
  - obowiązek zapewnienia należytej staranności przez cały cykl życia takich produktów.
- Rozporządzenie o cyberodporności ma wejść w życie w drugiej połowie 2024 r. (można spodziewać się jednak opóźnienia), a przez następne 3 lata zobowiązane podmioty będą miały czas na wprowadzanie na rynek unijny produktów zgodnych z nowymi przepisami.

Materiał powstał przy wsparciu Baker McKenzie.

3. METODOLOGIA BADAŃ

3.1.

Społeczeństwo 5.0, czyli zrównoważonego rozwoju dzięki technologii

METODOLOGIA BADAŃ / O BADANIU TECH4SOCIETY

METODOLOGIA

Badania online (CAWI) w ramach bloku pytań w Omnibusie GfK na panelistach GfK Access Panel

Wywiad do 10 minut

PRÓBA BADAWCZA

Reprezentatywna próba Polaków w wieku 18 -75 lat (próba reprezentatywna ze względu na płeć, wiek, wykształcenie, miejsce zamieszkania)

Liczebność próby: **N=1000**

REALIZACJA BADANIA

10-15 maja 2024 r.

CELE BADANIA

Określenie:

- strategicznych wyzwań stojących przed Polską,
- nastawienia do nowych technologii,
- technologicznego profilu polskiego społeczeństwa,
- otwartości na skorzystanie z nowych technologii.

PŁEĆ

49% 51%

WIEK

18-29	19
30-39	20
40-49	22
50-59	14
60-75	25

WYKSZTAŁCENIE

Podstawowe	14
Zasadnicze zawodowe	23
Średnie	37
Wyższe	26

MIEJSCE ZAMIESZKANIA

Wieś	40
Miasto do 50 tys.	24
Miasto do 500 tys.	24
Powyżej 500 tys.	12

REGION

Centralno-Środkowy	21
Północno-Wschodni	12
Północno-Zachodni	25
Południowo-Zachodni	24
Południowo-Wschodni	18

FAZA ŻYCIA

Młodzi do 34 lat bez dzieci	13
Rodzina z małymi dziećmi do 5 lat	14
Rodzina z dziećmi 6-14 lat	21
Rodzina z dziećmi 15-18 lat	8
Dorośli 35-49 bez dzieci 0-18	11
50-64 bez dzieci 0-18 pracują	10
50-64 bez dzieci 0-18 nie pracują	7
Emeryci 65+ bez dzieci 0-18	16

MIESIĘCZNE DOCHODY NETTO GOSPODARSTWA DOMOWEGO

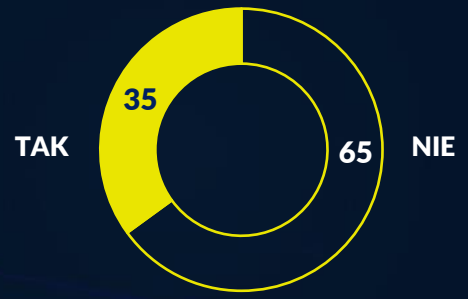
do 2000 PLN	5
2000-2999 PLN	3
3000-4499 PLN	15
4500 PLN i więcej	60
Odmowa podania	16

W wyniku zaokrągleń wskazania sumują się do 99%

WIELKOŚĆ GOSPODARSTWA DOMOWEGO

1 osoba	11
2 osoby	22
3 osoby	23
4 osoby	22
5 lub więcej osób	22

DZIECI DO LAT 18 W GOSPODARSTWIE DOMOWYM



ZMIANA METODY BADANIA Z CATI NA CAWI

W szóstej edycji badania (2024) zmieniono metodę zbierania danych z wywiadów realizowanych telefonicznie (CATI) na wywiady realizowane on-line (CAWI).

Zmiana metody badania zawsze wiąże się z różnicami w danych wynikających z czynników, które są trudne do kontrolowania, takich jak źródło próby, techniki kontroli danego wywiadu lub jakość respondentów, itp.

W związku z tym obserwowane zmiany w danych nie zawsze muszą wynikać z trendów rynkowych.

Jednak brak możliwości wprost porównania danych z edycji 2024 do serii danych z lat ubiegłych wynika przede wszystkim z:

- braku w pomiarze 2024 osób nie korzystających z Internetu,
- braku wpływu ankietera na udzielane odpowiedzi – respondenci w ankiecie CAWI mogą udzielać bardziej szczerych i anonimowych odpowiedzi, bo nie mają bezpośredniego kontaktu z ankieterem,
- różnych struktur demograficznych próby – struktura próby w tegorocznej edycji badania (2024) jest bardziej zbliżona do rzeczywistej struktury polskiego społeczeństwa pod względem wykształcenia.

3.2.

Cyberbezpieczeństwo oczami Polaków 2024

METODOLOGIA BADAŃ / O BADANIU CYBERSECURITY 2024

METODOLOGIA

Badanie online: wywiady CAWI realizowane online na GfK Access Panel

Wywiad do 15 minut

PRÓBA BADAWCZA

Reprezentatywna próba Polaków w wieku 18 -75 lat (próba reprezentatywna ze względu na płeć, wiek, wykształcenie, miejsce zamieszkania)

Liczebność próby: **N=1000**

REALIZACJA BADANIA

20-26 sierpnia 2024 r.

CELE BADANIA

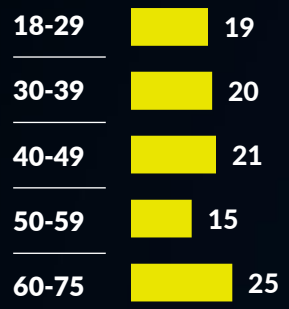
Określenie:

- wiedzy na temat cyberbezpieczeństwa,
- sposobów i popularności ataków i oszustw (scam),
- złych nawyków z zakresu cyberbezpieczeństwa,
- podejścia do przetwarzania i przechowywania danych oraz RODO (GDPR),
- doświadczania mowy nienawiści i opinii na temat ślepego pozwu,
- opinii na temat ochrony rodzicielskiej i dbania o bezpieczeństwo dzieci i młodzieży w internecie,
- nastawienia do kraju pochodzenia dostawców,
- stanu cyberbezpieczeństwa Polski.

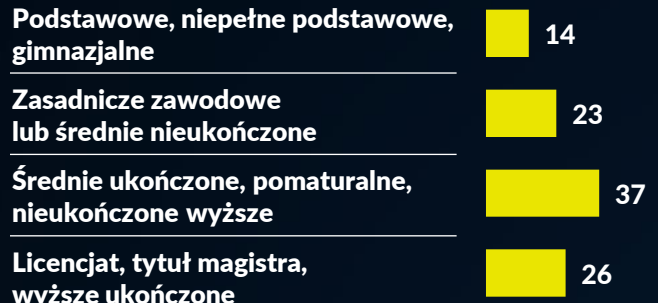
PŁEĆ

49% 51%

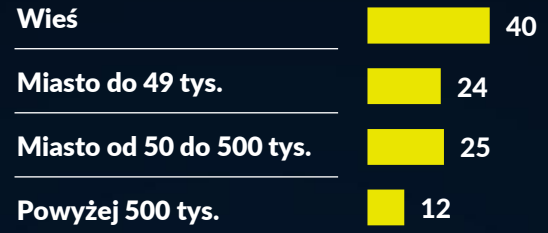
WIEK



WYKSZTAŁCENIE



MIEJSCE ZAMIESZKANIA

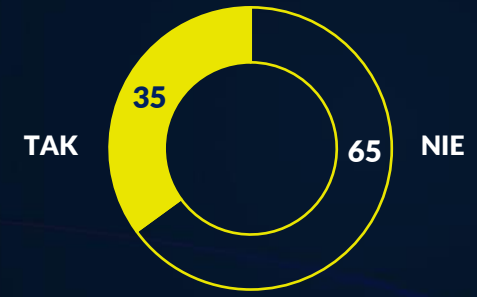


W wyniku zaokrągleń wskazania sumują się do 101%

MIESIĘCZNE DOCHODY NETTO GOSPODARSTWA DOMOWEGO

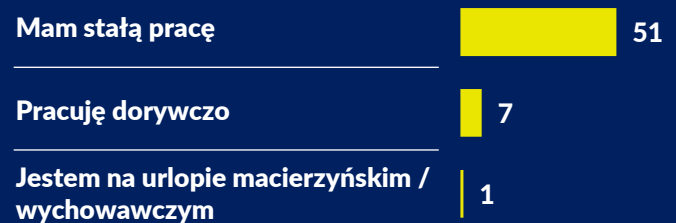
WIELKOŚĆ GOSPODARSTWA DOMOWEGO

DZIECI DO LAT 18 W GOSPODARSTWIE DOMOWYM



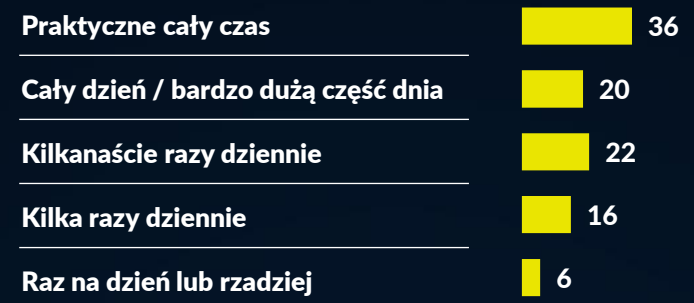
Dane w %

AKTUALNA SYTUACJA ZAWODOWA

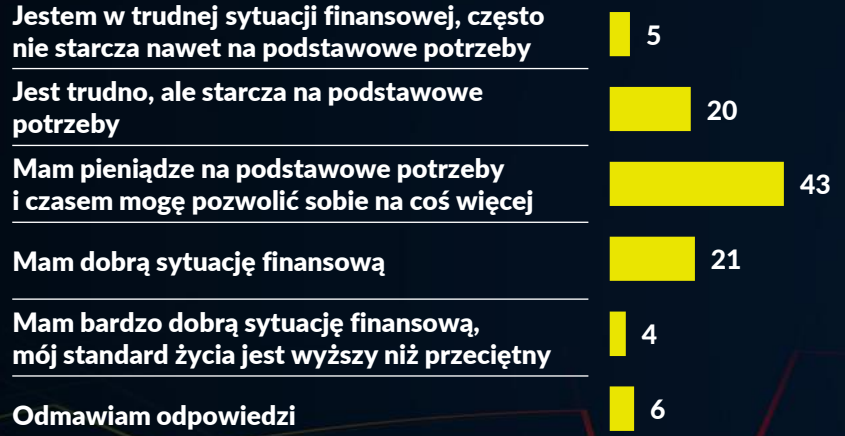


POSIADANE SŁUŻBOWE URZĄDZENIE

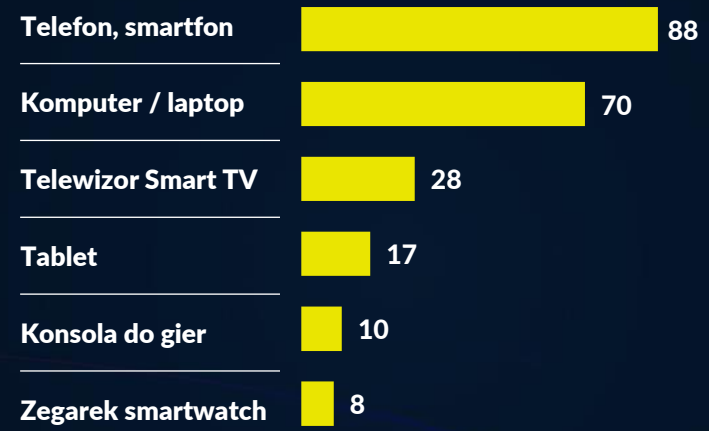
CZĘSTOTLIWOŚĆ KORZYSTANIA Z INTERNETU



SYTUACJA FINANSOWA



URZĄDZENIA, NA KTÓRYCH KORZYSTA Z INTERNETU



Dane w %

AUTORZY I EKSPERCI PUBLIKACJI

Piotr Mieczkowski

Dyrektor zarządzający, Członek zarządu fundacji Digital Poland,
Wiceprezes zarządu European AI Forum, Ekspert KIGEiT,
Członek grup roboczych przy Ministerstwie Cyfryzacji

Piotr ma ponad 20-letnie doświadczenie w realizacji projektów w sektorze nowych technologii. Obecnie zarządza pracami fundacji Digital Poland, która promuje cyfryzację jako element przewagi konkurencyjnej Polski. Jest wiceprezesem zarządu European AI Forum – największej organizacji europejskich spółek AI z siedzibą w Brukseli, jak również ekspertem Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji do spraw międzynarodowych, członkiem Komitetu Monitorującego FENG z ramienia Federacji Przedsiębiorców Polskich i członkiem grup roboczych przy Ministerstwie Cyfryzacji.

Piotr jest autorem lub współautorem raportów, publikacji, artykułów oraz polityk publicznych wspierających sektor nowych technologii, w tym sztucznej inteligencji (AI), internetu rzeczy (IoT), cyberbezpieczeństwa czy sieci 5G. Współtwórca strategicznego programu NCBR AI INFOSTRATEG, który wspiera wdrożenie AI w Polsce kwotą 840 mln zł.

Piotr posiada praktyczne doświadczenie w zakresie transformacji cyfrowej, tworzenia skutecznych polityk publicznych opartych na danych, procesów biznesowych, tworzenia programów edukacyjnych, doradztwa strategicznego czy projektowania rozwiązań ICT. Posiada aktualną wiedzę na temat takich zagadnień jak sztuczna inteligencja, duże zbiory danych, przetwarzanie w chmurze, internet rzeczy, sieci 5G czy inteligentne miasta.

Piotr pracował wcześniej w globalnej firmie doradczej (EY), w zintegrowanej grupie medialno-telekomunikacyjnej (Grupa Polsat Plus), operatorze sieci komórkowej (Orange) oraz w globalnej firmie energetycznej (Shell). Zrealizował z sukcesem ponad 35 projektów dla takich klientów jak Deutsche Telekom, E&, Liberty Global, Multimedia Polska, Netia, Orange, Telenor, T-Mobile, Saudi Telekom Company, Solutions by STC, UPC, Vodafone. Piotr pracował również dla regulatorów w regionie CEE, np. UKE, NMHH, GNCC, SPRK, RRT oraz kluczowych decydentów, np. Ministerstwa Cyfryzacji w Polsce, izb branżowych np. KIGEiT, PIIT czy agencji grantowych np. NCBR. Realizował również projekty doradcze m. in. we współpracy Artur D. Little, BCG czy EY-Parthenon.

Jest absolwentem Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej oraz Wydziału Zarządzania Uniwersytetu Warszawskiego. Posiada szereg specjalistycznych certyfikatów technicznych i menedżerskich.

W swoich działaniach skupia się na współpracy, budowaniu aktywnych społeczności i przede wszystkim na wypracowywaniu konkretnych wyników na bazie faktów i danych.

dr inż. Elżbieta Andrukiewicz
Instytut Łączności – Państwowy Instytut Badawczy

dr Michał Boni
Fundacja Digital Poland, Uniwersytet SWPS

Renata Gluza
TVN Warner Bros. Discovery

Anna Goławska
Fujitsu Technology Solutions

dr Urszula Góral
Uniwersytet Kardynała Stefana Wyszyńskiego, Kancelaria Sejmu RP

Adam Haertle
ZaufanaTrzeciaStrona.pl

dr Agnieszka Jankowska
Fundacja Digital Poland, T-Mobile Polska

Renata Kania
T-Mobile Polska

Michał Kielczyk
Polpharma

Małgorzata Kilian-Grzegorczyk
Stowarzyszenie Demagog

Piotr Konieczny
Niebezpiecznik.pl

Łukasz Kozłowski
Federacja Przedsiębiorców Polskich

Michał Kurek
KPMG

dr Konrad Maj
Uniwersytet SWPS

gen. bryg. rez. Włodzimierz Nowak
Niezależny ekspert

Katarzyna Nowicka
Stowarzyszenie Twoja Sprawa

Radosław Nożykowski
Baker McKenzie

dr Łukasz Olejnik, LL.M
prywatnik.pl

Jan Oleszczuk-Zygmuntowski
Polska Sieć Ekonomii

Konrad Płachecki
Bank Gospodarstwa Krajowego

Robert Pławiak
Polpharma

Anna Rywczyńska
NASK

dr hab. Agnieszka Skala, prof. PW
Politechnika Warszawska

dr hab. Urszula Soler, prof. KUL
Katolicki Uniwersytet Lubelski

dr Małgorzata Starczewska-Krzysztoszek
Uniwersytet Warszawski

Ksawery Stojak
Bank Gospodarstwa Krajowego

Anna Strężyńska
KIGEiT

Ignacy Święcicki
Polski Instytut Ekonomiczny

Izabela Taborowska
Cyberclue

Tomasz Zieliński
InformatykZakladowy.pl

Mateusz Zubkowicz
GfK

Robert Zyskowski
Symfonia

dr inż. Jerzy Żurek
Asseco, Netia

Ekspertki i eksperci, którzy znacząco przyczynili się do powstania kwestionariusza pozwalającego zbadać cyberbezpieczeństwo oczami Polaków.

Renata Gluza | TVN Warner Bros. Discovery | Konkret24
Anna Goławska | Fujitsu Technology Solutions
Michał Kielczyk | Polpharma
Radosław Nożykowski | Baker McKenzie w Polsce
Robert Pławiak | Polpharma
Wioletta Rylska | GfK
Paweł Terpilowski | Stowarzyszenie Demagog
Lidia Ustasiak-Stępińska | T-Mobile Polska
Anna Węgrzynowicz | Bank Gospodarstwa Krajowego
Mateusz Zubkowicz | GfK

O PARTNERACH RAPORTU

Bank Gospodarstwa Krajowego to polski bank rozwoju, jedyna taka instytucja w Polsce. BGK wspiera zrównoważony rozwój społeczno-gospodarczy kraju. Jego działania przyczyniają się do tworzenia miejsc pracy, budowy mieszkań, rozwoju infrastruktury i poprawy jakości powietrza. Bank dba o przyszłe pokolenia – buduje kapitał społeczny, rozwija przedsiębiorczość i zapewnia odpowiedzialne finansowanie. Jest obecny w każdym regionie Polski, a także za granicą – ma swoje przedstawicielstwa w Londynie, Brukseli i Frankfurcie nad Menem. Bank aktywnie uczestniczy we wdrażaniu Funduszy Europejskich w Polsce, jak również produktów finansowanych z Krajowego Planu Odbudowy. BGK wspiera eksport i ekspansję zagraniczną polskich firm. Ponadto, bank angażuje się w rozwój gospodarki cyfrowej, wspierając cyfryzację przedsiębiorstw oraz oferując dedykowane narzędzia finansowe. Poprzez współpracę z biznesem, sektorem publicznym i instytucjami finansowymi, odpowiadana potrzeby gospodarcze oraz podejmuje szereg inicjatyw promujących zrównoważony rozwój.

An NIQ Company

Od 90 lat klienci na całym świecie ufają nam, że dostarczymy im oparte na danych odpowiedzi na kluczowe pytania dotyczące ich procesów decyzyjnych.

Wspieramy ich rozwój dzięki naszemu kompleksowemu zrozumieniu zachowań konsumenckich i dynamiki, która wpływa na rynki, marki i trendy medialne.

W 2023 r. liderzy branży GfK i NielsenIQ połączyli się, aby zaoferować swoim klientom największy zasięg globalny.

Dzięki holistycznemu spojrzeniu na handel detaliczny i najbardziej kompleksowej wiedzy o konsumentach, dostarczanej przez analizy na najnowocześniejszych platformach, GfK napędza „wzrost dzięki wiedzy”.

Więcej informacji można znaleźć na stronie gfk.com.

O FUNDACJI DIGITAL POLAND I DIGITAL FESTIVAL 2024

digitalpoland

O Fundacji Digital Poland

Jako organizacja non-profit fundacja podejmuje działania, aby Polska stała się jednym z głównych światowych centrów innowacji cyfrowych. Poprzez swoje działania przekształca cyfrowe wyzwania stojące przed Polską w szanse dla rodzimej gospodarki. Bez aktywnego udziału społeczeństwa rozwój technologiczny i cyfrowy naszego kraju się nie powiedzie, dlatego założyciele fundacji stawiają przede wszystkim na edukację, organizując szereg wydarzeń czy akcji edukacyjnych, takich jak Digital Fitness Test, Digital Ars, Akademia SkillUp, Digital Festival czy Noc Innowacji, promując przy tym nowe technologie w życiu codziennym i biznesie. W oczach zagranicznych inwestorów fundacja prezentuje Polskę jako miejsce do prowadzenia działalności badawczo-rozwojowej i opracowywania innowacji o zasięgu międzynarodowym, korzystając z umiejętności naszych specjalistów ICT.

Fundacja prowadzi szeroką działalność w zakresie analiz spraw publicznych, współtworząc największy w Polsce zestaw rekomendacji „Czas na cyfrową gospodarkę". Fundacja realizuje też szereg badań konsumentów i firm, publikując przy tym nawet kilkanaście bezpłatnych opracowań rocznie, np. w zakresie wiedzy Polaków na temat dezinformacji czy subskrypcji. Fundacja jest też jednym z założycieli European AI Forum w Brukseli – największej w Europie organizacji skupiającej firmy i organizacje z zakresu sztucznej inteligencji (więcej na eaiforum.org).

We wszystkich swoich działaniach fundacja stawia przede wszystkim na współpracę, tworząc sieć kontaktów i bliskich relacji, bo tylko dzięki współpracy i otwartości na innych jesteśmy w stanie uczynić Polskę jednym z wiodących na świecie centrów innowacji cyfrowych. Fundacja zaprasza do współpracy wszystkie osoby zainteresowane realizacją projektów edukacyjnych, innowacyjnych czy z zakresu polityk publicznych, które pozytywnie zmienią polską gospodarkę. Wśród fundatorów i partnerów strategicznych są takie firmy, jak: Baker McKenzie, Fujitsu, Lenovo, Polpharma, Play, Ringier Axel Springer Polska, Symfonia, T-Mobile Polska, TVN Warner Bros. Discovery czy Visa. Partnerami fundacji Digital Poland są m.in. firmy Prowly, Ströer oraz Techland.

Chcesz dowiedzieć się więcej? Odwiedź digitalpoland.org

STRATEGICZNI FUNDATORZY I STRATEGICZNI PARTNERZY

Baker McKenzie.

FUJITSU

Lenovo

PLAY

polpharma

ringier axel springer

symfonia

T

tvn | WARNER BROS. DISCOVERY

VISA

PARTNERZY

Prowly

STRÖER

TECHLAND®

digitalpoland

Międzybranżowa, ogólnokrajowa inicjatywa skupiająca się na wynikach naszych działań

Współdzielimy i prowadzimy inicjatywy i koalicje cyfrowe, współpracujemy, tworzymy sieć kontaktów i promujemy cyfryzację w wiodących mediach

Pomagamy przekształcać cyfrowe wyzwania w szanse dla polskiej gospodarki i społeczeństwa poprzez tworzenie najlepszych polityk cyfrowych

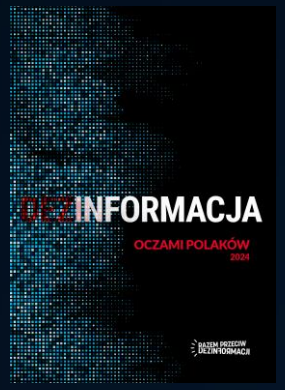
Promujemy Polskę jako wiodący ośrodek innowacji cyfrowych

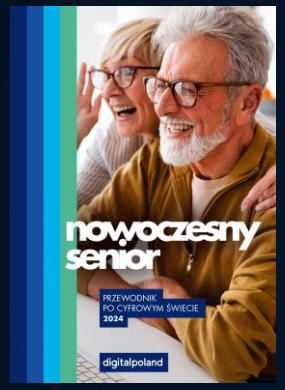
Edukujemy społeczeństwo, prezentujemy fakty, obalamy mity, podpowiadamy jak korzystać z nowych technologii

Mamy udokumentowane osiągnięcia. Przykłady naszych inicjatyw.

- Digital Festival
- Digital Shapers
- Polityki cyfrowe
- Czas na cyfrową gospodarkę
- AI Hub
- European AI Forum
- Koalicja „Cyfrowi Seniorzy”
- Think Tank
- Study Tours
- Koalicja „Razem przeciw dezinformacji”
- Digital CEO
- Digital Champions CEE
- Digital Fitness Test
- Digital Summit
- Polska jako centrum R&D
- Akademia SkillUp

Wspólnie z partnerami prowadzimy działalność edukacyjną i badawczą. Jesteśmy niezależnym think-tankiem. Pobierz bezpłatnie wszystkie nasze materiały ze strony fundacji po uprzedniej rejestracji.





Digital Festival

European Digital Days

6. edycja
1.10.-10.11.2024

www.digitalfestival.pl

Digital Festival

Włącz się w Digital Festival 2024!

6 tygodni pełnych różnorodnych inicjatyw i wydarzeń, z których każdy może bezpłatnie skorzystać

01.10-10.11.2024

Akademia SkillUp

Zrób jedno ze stu szkoleń, które wprowadzą Cię do cyfrowego świata
Zrób szkolenie

Cyfrowe historie

Zainspiruj się wywiadami z osobami które odniosły sukces, dzięki digitalowi lub w digitalu

Digital Ars

5. edycja pierwszego w Polsce konkursu na sztukę tworzoną przy wsparciu AI
Zgłoś pracę

Digital Fitness Test

5. edycja pierwszego w Polsce testu z umiejętności cyfrowych, który powstał we współpracy z KE. Dostępny dla dzieci i dorosłych
Zrób test

Nowoczesny Senior

Cyfryzacja nie zna wieku! Każdy jest seniorem, tyle że „jutro". Wykorzystaj możliwości cyfrowego świata dzięki 4. edycji akcji Nowoczesny Senior
Pobierz przewodnik

Noc Innowacji

Poznaj od kuchni nowe technologie zmieniające świat. Weź udział w darmowych pokazach i warsztatach EY GDS w dniu **18.10.2024**

Strefa Wiedzy

200+ artykułów, 70+ podcastów, 17+ raportów i poradników w zasięgu Twojej ręki! Dowiesz się więcej o cyfrowym świecie!
Wejdź do strefy wiedzy

Tech4Society

Kompleksowy raport o cyberbezpieczeństwie oczami Polaków oraz puls Społeczeństwa 5.0
Przeczytaj

Test Dojrzałości Cyfrowej

Zbadaj poziom dojrzałości cyfrowej Twojej firmy i zaplanuj jej transformację. Test powstał we współpracy z PFR
Wykonaj test

Wydarzenia

Weź udział w wartościowym networkingu i spotkaniach dotyczących cyfryzacji i technologii

Digital Festival EDD European Digital Days _2023

Tak było w 2023!

6
tygodni edukacji o AI

200+
partnerów

130+
wydarzeń online/offline

dotarliśmy do
11+ mln
osób w mediach ogólnopolskich

dotarliśmy do
4,6+ mln
osób w mediach społecznościowych

Nowoczesny Senior

rozesłaliśmy
13,6 tys.
poradników „Nowoczesny senior” online oraz drukowanych

30+ tys.
przeszkolonych seniorów

52,3 mln
zasięg informacji

Digital Fitness Test

11,2+ tys.
osób wykonało quiz

Noc Innowacji

16
miast

100+
wydarzeń

11,7+ tys.
uczestników

112,5 mln
zasięg informacji

Strefa wiedzy

15+
wideopodcastów

20
artykułów o AI

Akademia SkillUp

90+
szkoleń