KRAJOWY PLAN ODBUDOWY

Rzeczpospolita Polska

Sfinansowane przez Unię Europejską NextGenerationEU

WOJEWÓDZTWO POMORSKIE

Bezpieczna przestrzeń ONLINE

Kamila Dąbrowska

Dezinformacja i ataki w sieci

Twój przewodnik po cyfrowym przetrwaniu

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

POMORSKIE KOMPETENCJE JUTRA

FUNDACJA NIE WIDAĆ PO MNIE

Tytuł: Dezinformacja i ataki w sieci. Twój przewodnik po cyfrowym przetrwaniu
Autor: Kamila Dąbrowska

Nadzór merytoryczny: Magdalena Gawżyński, Aigorythmics Sp. z o.o.
Korekta: Urszula Szybowicz
Korekta składu: Urszula Szybowicz
Skład i opracowanie graficzne: Kamila Olejnik
Zdjęcia: źródło - baza zdjęć iSTOCK
ISBN: 978-83-68385-37-3

Przygotowanie merytoryczne i graficzne materiałów:
Ul. Okopowa 58/72, lok 604, Klif Tower
01-042 Warszawa

Projekt realizowany jest w ramach naboru: “Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych. “

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych” **jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.**

Warszawa 2026

Spis treści, czyli o tym, czego możesz się spodziewać

Wstęp – Dlaczego to dotyczy również Ciebie?

- Zhakowanie emocji to cenne hasło do systemu

Anatomia kłamstwa – dezinformacja 2.0

- Czym różni się fake news od deepfake'u?
- Mechanizm „emotional hacking" – dlaczego najłatwiej wierzymy w to, co nas złości?

Inteligentne ataki, których nie widzisz

- Metody socjotechniczne, czyli jak oszuści kradną Twoją tożsamość?
- Bezpieczeństwo konta. Dlaczego 2FA to absolutne minimum?

Wsparcie psychologiczne – kiedy hejt lub dezinformacja uderzają w zdrowie psychiczne

- Mechanizm oszustwa, czyli efekt iluzorycznej prawdy
- Skala problemu: nie jesteś w tym sam(a)
- Dlaczego to boli (i dlaczego to normalne)?

Twoje cyfrowe BHP

- Czy jesteś bezpieczny/bezpieczna w sieci?
- Manifest świadomego użytkownika

Cyfrowa apteczka, czyli gdzie zgłaszać oszustwa i ataki cyfrowe?

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Wstęp: Dlaczego to dotyczy również Ciebie?

Cześć!
Skoro to czytasz, to znaczy, że właśnie wygrałeś ze swoim algorytmem. To niezwykle ważne, że wybrałeś ten e-book, zamiast scrollować dziesiątki przypadkowych treści, które masz na wyciągnięcie ręki.

Masz w kieszeni narzędzie, o jakim Twoi rodzice mogli tylko pomarzyć. Dostęp do internetu to Twoje naturalne środowisko. To tu budujesz tożsamość, relacje i podejmujesz decyzje, które potem przenosisz do „realu". Ale właśnie dlatego, że jesteś tu tak aktywny, jesteś na celowniku technologii manipulacji.

„Mnie to nie dotyczy, ogarniam sieć lepiej niż starzy" – pomyślałeś? Właśnie wpadłeś w pułapkę. To złudzenie trzeciej osoby (z ang. third-person effect). Większość z nas wierzy, że manipulacja dotyczy „innych", a my jesteśmy na nią odporni. Tymczasem prawda jest brutalna: to Twoje pokolenie jest na pierwszej linii frontu dezinformacji. Co gorsza, statystyki pokazują, że młodzi rzadko reagują na fejki. Często szkoda Wam na to czasu lub uważacie, że to nie Wasza sprawa.

W tym poradniku pokażemy Ci, że cyfrowa biegłość (to, jak szybko klikasz w apkach) to nie to samo co cyfrowa odporność. Ta druga zaczyna się tam, gdzie kończą się nawyki, a pojawia świadomość zagrożeń. Chcemy pokazać Ci mechanizmy działające w tle, byś odzyskał swoje najsilniejsze narzędzie: krytyczne myślenie. W świecie, który nigdy się nie wylogowuje, to Twoja jedyna prawdziwa ochrona.

Te liczby mogą zrobić na Tobie wrażenie:

- W 2024 roku w całej Unii Europejskiej odsetek młodych ludzi korzystających z internetu codziennie wyniósł średnio aż **97%**. W niektórych krajach to okrągłe **100%!** Kawa na ławę: Internet przestał być dodatkiem do życia – on jest jego częścią, tak samo jak Twoje wyjście do szkoły czy spotkanie na mieście.[1]

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

- Statystyczny polski nastolatek spędza w Internecie średnio **5 godzin i 36 minut dziennie** (i to tylko w dni powszednie!). To oznacza, że w ciągu roku oddajesz ponad 85 pełnych dób ze swojego życia. To tak, jakbyś spędził prawie 3 miesiące bez przerwy, gapiąc się w ekran.[2]

- Codziennie **skrolujesz około 100 metrów treści**.[3] To tak, jakbyś codziennie wbiegał na szczyt 30-piętrowego wieżowca, mijając po drodze tysiące billboardów.

- Co czwarty z Was (25,8%) ogarnia jednocześnie od **5 do 8 kont na różnych platformach**. Mało? To teraz trzymaj się mocno: ponad 1/3 (36%) Twoich rówieśników ma ich więcej niż 8! Jesteś wśród nich?[2]

- YouTube i TikTok to obecnie absolutni rekordziści – bez względu na to, ile masz lat i z jakiego sprzętu korzystasz, to właśnie te apki są największymi „pochłaniaczami czasu" w Polsce.[4]

- Myślisz, że patostreamy to tylko nieszkodliwy żart, rozrywka? Statystyki są bezlitosne: co czwarty z Was **(25,8%) ogląda transmisje pełne wulgaryzmów, przemocy i obscenicznych zachowań.** Dlaczego to niebezpieczna pułapka? Takie nacechowane agresją transmisje internetowe i widowiska to nic innego, jak „dezinformacja emocjonalna". [2]

- Badania Stanford University pokazały, że aż **80% młodych ludzi nie potrafi odróżnić treści reklamowej od prawdziwego newsa**, choć są pewni swoich umiejętności.[5]

- Szacuje się, że jeszcze w tym roku aż **90% treści w internecie może być w jakiś sposób modyfikowanych przez sztuczną inteligencję (AI).**[6]

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Zhakowanie emocji to cenne hasło do systemu

Skoro już wiesz, ile czasu spędzasz w sieci, czas zadać sobie pytanie: dlaczego tak trudno jest odłożyć telefon? To nie jest kwestia Twojej „słabej woli". Przeciwko Tobie stoją najpotężniejsze światowe algorytmy, projektowane przez sztaby psychologów i inżynierów. Ich jedynym zadaniem jest utrzymać Cię przed ekranem choćby o sekundę dłużej.

Dla wielkich platform Twoja uwaga to waluta. Dosłownie. Dziś już nie ma anonimowości w sieci! Wykorzystanie Big Data przez platformy takie jak Meta czy Google umożliwia precyzyjne profilowanie użytkowników. Dzięki narzędziom analitycznym i reklamowym, korporacje te zbierają kompleksowe dane, które służą do Twojej jednoznacznej identyfikacji w sieci.

Im dłużej patrzysz, tym więcej reklam widzisz, tym więcej danych o sobie zostawiasz i tym więcej zarabiają korporacje. Aby tę walutę zdobyć, twórcy technologii używają Twoich własnych emocji jako haczyka. A firmy technologiczne, politycy i oszuści walczą o to, żebyś kliknął, udostępnił lub kupił ich narrację. Robią to, hakując nie Twoje hasło, ale Twoje emocje.

Pułapka „nieskończonego scrollowania"

Zauważyłeś, że TikTok, YouTube Shorts czy Instagram nigdy się nie kończą? Mechanizm nieskończonego przewijania (z ang. infinite scroll) został zaprojektowany na wzór automatów do gier w Las Vegas.

Jak to działa? Nie wiesz, co zobaczysz za moment. Może to być nudny film, a może totalny hit (coś trendującego), który Cię rozśmieszy, wzruszy. Ten element niepewności sprawia, że Twój mózg uwalnia dopaminę przy każdym przesunięciu palca. Czekasz na fajny content, a algorytm dawkuje Ci go tak, żebyś nie mógł przestać.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Clickbait emocjonalny, bo to właśnie on sprzedaje się najlepiej

Niestety algorytmy nie promują treści, które są prawdziwe lub wartościowe. Promują te, które budzą najsilniejsze emocje.

- Prosty przykład: post o tym, że ktoś był na wakacjach na Sycylii zdobędzie polubienia. Ale post o tym, że ktoś znany powiedział coś skandalicznego o Twojej ulubionej grze/zespole, wywoła już burzę w komentarzach.

- Kolejny przykład: wyobraź sobie, że scrollujesz feed i nagle widzisz czarno-białe, ziarniste zdjęcie Twojego ulubionego twórcy lub znanej osoby. Fotografia jest lekko nieostra, on ma spuszczony wzrok, a obok widnieje krótki, urwany napis: „To koniec…" albo „Nie sądziliśmy, że to się tak skończy". Co czujesz? Nagłe ukłucie w brzuchu, niepokój, lęk o tę osobę. Twój mózg natychmiast podpowiada najczarniejszy scenariusz: wypadek, śmierć, choroba.

  A jaka jest rzeczywistość? Klikasz w panice, a tam… reklama nowego kursu, zapowiedź wyprzedaży albo informacja, że influencer robi sobie tydzień przerwy od social mediów. Kurtyna.

- Na co uważać? Jeśli czujesz się oszukany, towarzyszy Ci złość lub chęć natychmiastowego odpisania na taką treść, to właśnie zostałeś zmanipulowany/zmanipulowana przez algorytm. Twoje oburzenie to dla platformy po prostu „wysoki poziom zaangażowania".

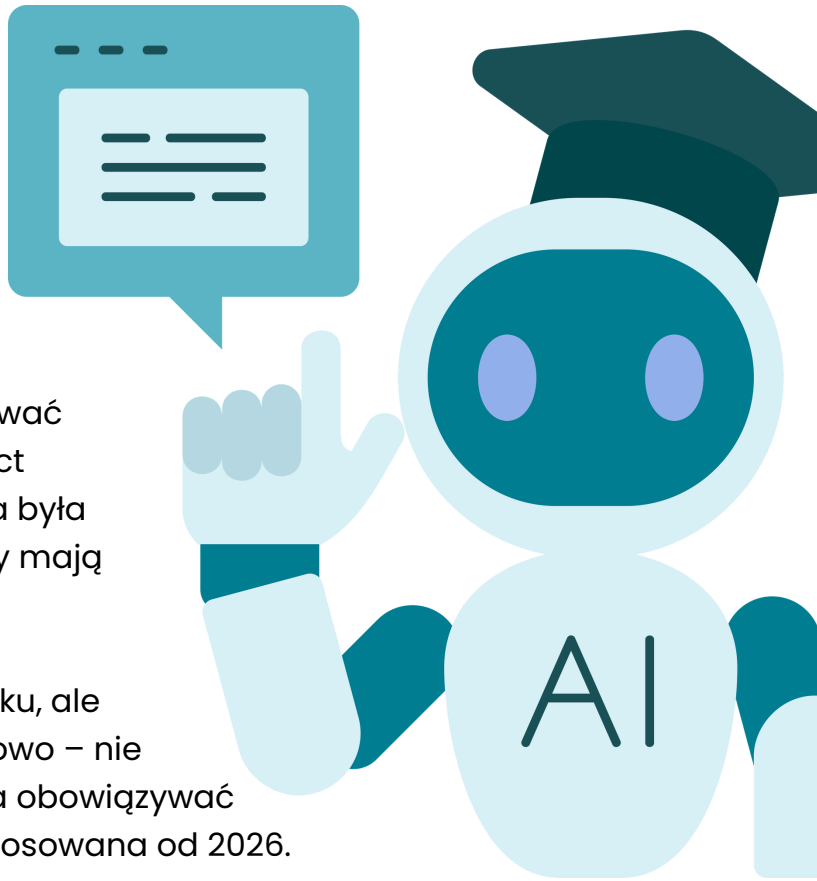
Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Deepfake, „idealni" influencerzy i AI

To już nie są wyłącznie filtry wygładzające cerę. Wkraczamy w erę, w której postać, którą śledzisz, może w ogóle nie istnieć lub promować rzeczy, których nigdy nie widziała na oczy, które nie są realne.

- Przykład takiej manipulacji, proszę bardzo: coraz częściej spotykamy tzw. virtual influencers – wygenerowane przez AI postacie, które wyglądają jak Twoi rówieśnicy. Nie męczą się, nie mają gorszych dni i zawsze wyglądają perfekcyjnie w ubraniach, które reklamują.
- Jakie płynie z tego zagrożenie? Porównujesz swoje prawdziwe życie do matematycznie wyliczonego ideału. To prosta droga do spadku samooceny, za którą idzie chęć „naprawienia się" poprzez zakupy produktów, których nie potrzebujesz.

Czy wiesz, że...



W Unii Europejskiej powstały nowe przepisy dotyczące sztucznej inteligencji, nazywane AI Act (Rozporządzenie UE 2024/1689). To pierwsze takie prawo na świecie, które reguluje, jak można tworzyć i używać systemów AI. Najprościej mówiąc: AI Act ma sprawić, żeby sztuczna inteligencja była bezpieczna i żeby ludzie wiedzieli, kiedy mają z nią do czynienia.

AI Act wszedł w życie 1 sierpnia 2024 roku, ale jego przepisy są wprowadzane stopniowo – nie wszystko działa od razu. Część zaczęła obowiązywać w 2025 roku, a całość będzie w pełni stosowana od 2026.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

POMORSKIE KOMPETENCJE JUTRA
FUNDACJA NIE WIDAĆ PO MNIE

Dzięki tym przepisom:

- firmy muszą informować, gdy rozmawiasz z AI (np. chatbotem),
- treści stworzone przez AI w niektórych przypadkach (np. deepfake'i) muszą być oznaczone,
- systemy AI, które mogą być niebezpieczne (np. w medycynie czy rekrutacji), podlegają surowszym zasadom.

To nie jest zakaz korzystania z AI - wręcz przeciwnie. Chodzi o to, żebyś nie był(a) wprowadzany(a) w błąd i miał(a) jasność, co jest stworzone przez człowieka, a co przez „maszynę".

W praktyce oznacza to, że Internet ma być bardziej „uczciwy": jeśli coś wygląda jak prawdziwa osoba albo wiadomość, powinieneś mieć możliwość sprawdzenia, czy nie zostało wygenerowane przez sztuczną inteligencję. 11

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

FOMO i ograniczone czasowo okazje

Pewnie orientujesz się, że z ang. fear of missing out, to strach, że coś Cię ominie, ale czy rozumiesz, że to nic innego, jak paliwo dla marketingu. Niby mamy tego świadomość, a nadal dajemy się podejść tej socjotechnice i pozwalamy włamywać się do systemu naszych emocji.

- Jak Cię łapią? Liczniki czasu przy promocjach na skiny w grach, dropy ubrań dostępne wyłącznie przez 15 minut, czy powiadomienia typu „Twoja znajoma właśnie dodała relację, zobacz ją, zanim zniknie".

- Efekt? Podejmujesz decyzje impulsywnie, pod wpływem stresu, a nie chłodnej kalkulacji. Twoje pieniądze (lub pieniądze Twoich rodziców) płyną szerokim strumieniem tam, gdzie skieruje je sprytnie wywołany lęk.

Zapamiętaj prostą zasadę, w świecie cyfrowym, jeśli nie płacisz za produkt, to Ty jesteś produktem. Twoje emocje – strach, radość, złość – są analizowane i pakowane w paczki danych, które potem kupują firmy, by jeszcze skuteczniej przykuć Cię do ekranu.

Jak nie dać się zhakować?

Cyfrowa odporność to świadomość, że każde „darmowe" kliknięcie ma swoją cenę. Nie chodzi o to, żebyś usunął/usunęła wszystkie apki. Chodzi o to, żebyś to Ty trzymał(a) telefon, a nie telefon trzymał Ciebie.

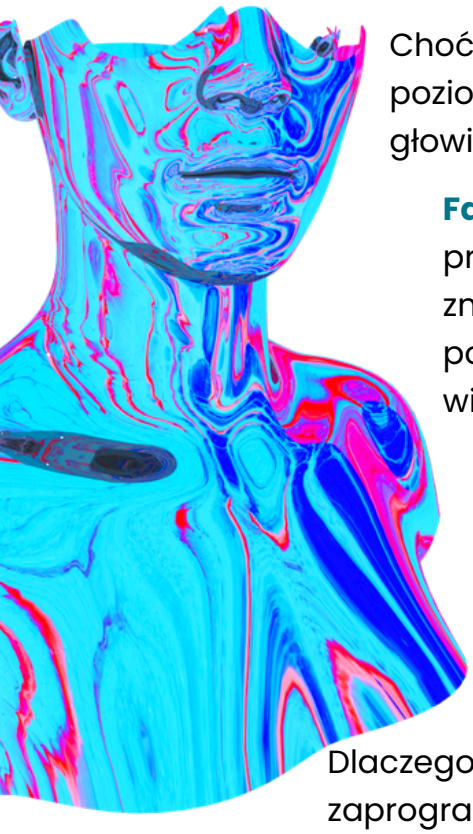
Dobrze wiesz, że nowoczesne technologie to już nie tylko gadżety, ale integralna część naszej codzienności, dlatego nie chodzi o to, byś się od nich radykalnie odcinał(a) (chyba, że masz taką potrzebę), ale by wyposażyć się w cyfrową tarczę. Kluczowe jest korzystanie z sieci świadomie, krytycznie i bezpiecznie. To pozwala na zachowanie równowagi między światem online a życiem w realu. **– podsumowuje psycholog Marek z Fundacji Nie Widać Po Mnie.**

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Anatomia kłamstwa – dezinformacja 2.0

Myślisz, że dezinformacja to po prostu „kłamanie w internecie"? Tymczasem to precyzyjnie zaprojektowana broń, która korzysta z najnowszych technologii i słabości ludzkiej psychiki. To nie jest amatorskie pisanie bzdur – to zaawansowana inżynieria społeczna.

Czym różni się fake news od deepfake'u?



Choć oba mają Cię oszukać, działają na zupełnie innych poziomach. Warto znać różnicę, żeby wiedzieć, który „detektor" w głowie włączyć.

Fake News: to fałszywa informacja ubrana w szaty prawdziwego newsa. Może to być zmyślony artykuł, zmanipulowany cytat wyjęty z kontekstu lub stare zdjęcie podpisane jako „zdarzenie z dzisiaj". Fake news atakuje Twoją wiedzę. Żeruje na tym, że nie sprawdzisz źródła.

Deepfake: to wyższy poziom wtajemniczenia. Tutaj do gry wchodzi sztuczna inteligencja (AI). Deepfake to realistyczne wideo lub nagranie audio, na którym osoba mówi lub robi rzeczy, których w rzeczywistości nigdy nie wypowiedziała ani nie zrobiła.

Dlaczego to groźne? Bo Twój mózg jest ewolucyjnie zaprogramowany, by wierzyć własnym oczom i uszom. Deepfake atakuje Twoje zmysły. Nawet jeśli wiesz, że taka technologia istnieje, Twoja podświadomość i tak wysyła sygnał: „Przecież widzę, że on to mówi!".

Krótka piłka: fake news to kłamstwo, które musisz przeczytać. Deepfake to kłamstwo, które musisz przeżyć.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

POMORSKIE KOMPETENCJE JUTRA
FUNDACJA NIE WIDAĆ PO MNIE

Mechanizm „emotional hacking" – dlaczego najłatwiej wierzymy w to, co nas złości?

Zastanawiałeś/zastanawiałaś się kiedyś, dlaczego w sieci najszybciej rozchodzą się treści, które wywołują dramę, kłótnie i wściekłość? Za tym stoi wspomniany „emotional hacking", czyli emocjonalna manipulacja. To nic innego jak najlepsze narzędzie do omijania cyfrowych zabezpieczeń. Ich celem jest paraliżowanie, maksymalne skupienie Twojej uwagi, aż po zaciekawienie, czy stworzenie fałszywego poczucia pilności.

Algorytmy i twórcy (czasem tzw. farmy trolli) dezinformacji, wykorzystując ludzkie emocje, posługują się podstawową a zarazem kluczową wiedzą. Rozumieją, że nasza kora przedczołowa (odpowiedzialna za logiczne myślenie) wyłącza się, gdy do głosu dochodzą silne emocje, dlatego w nie uderzają.

Wystarczy przyjrzeć się gniewowi, który staje się autostradą do Twojego mózgu. Kiedy widzisz coś, co Cię ekstremalnie złości (np. tytuły: „Ten polityk jest przeciwko umowom śmieciowym!" albo „Szokujące zachowanie nastolatków w Twoim mieście!"), T wój organizm przechodzi w tryb „walcz lub uciekaj". Efekt? Zamiast sprawdzić, czy to prawda, natychmiast klikasz „udostępnij", komentujesz lub przesyłasz dalej znajomym. Chcesz ostrzec innych lub wyrazić swój sprzeciw. W tym momencie przestałeś być użytkownikiem, a stałeś się darmową tubą kłamstwa. Niech pierwszy rzuci kamieniem, kto nie przegląda informacji, bazując wyłącznie na tytułach artykułów, a nie ich prawdziwej treści.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

POMORSKIE KOMPETENCJE JUTRA
FUNDACJA NIE WIDAĆ PO MNIE

Kiedy codziennie wpadasz na negatywne treści, Twój mózg otrzymuje sygnały o niebezpieczeństwie, co eskaluje w Tobie ogromne napięcie i stres. Algorytmy tylko podkręcają ten stan – są zaprogramowane tak, by serwować to, co najbardziej Cię porusza. Pamiętaj, że to nie Ty masz problem z emocjami, to technologia próbuje je zhakować, byś nie mógł /mogła odłożyć telefonu. – tłumaczy psycholog Marek.

Dlaczego w to wierzysz?

Bo dezinformacja zawsze uderza w Twoje wartości. Jeśli w coś mocno wierzysz, a ktoś podsunie Ci dowód (nawet fałszywy), który potwierdza Twoje obawy – Twój mózg przyjmie to bez krytyki. To tzw. efekt potwierdzenia. Pamiętaj, twórcy fake newsów nie chcą, żebyś myślał(a). Oni chcą, żebyś czuł(a). Bo człowiek, który czuje silny gniew, jest najłatwiejszy do sterowania.

Do emocji i wartości dochodzi jeszcze jeden, zabójczy czynnik: tempo, w jakim żyjesz. Scrollujesz w kolejce po kawę, w autobusie, między lekcjami, a nawet idąc chodnikiem (pamiętaj, że nie powinieneś tego robić na przejściu dla pieszych). Masz zaledwie 2-3 sekundy na ocenę posta, zanim palec przesunie ekran dalej. W tym tempie Twój mózg przełącza się na „tryb oszczędzania energii". Zamiast analizować fakty, szuka skrótów.

Zadanie dla Ciebie: następnym razem, gdy zobaczysz post, który sprawi, że poczujesz nagłą ochotę, by „wyjść z siebie i stanąć obok", omiń go, zaznacz okienko, że Cię nie interesuje. Nakarm swój algorytm informacją, że nie akceptujesz treści, które wywołują tak impulsywne emocje.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

POMORSKIE KOMPETENCJE JUTRA
FUNDACJA NIE WIDAĆ PO MNIE

Inteligentne ataki, których nie widzisz

Większość z nas wyobraża sobie hakera jako gościa w ciemnej bluzie, który wpisuje zielone linijki kodu. W praktyce wiele współczesnych ataków wcale nie polega na „włamaniu się" do systemu, tylko na nakłonieniu Cię do podjęcia złej decyzji.

Dziś cyberatak często zaczyna się od zwykłej wiadomości:

- maila, który wygląda jak od banku,
- SMS-a z „pilną dopłatą",
- albo wiadomości od „znajomego", który prosi o przelew.

Jeszcze kilka lat temu takie próby łatwo było rozpoznać - błędy językowe, dziwne formatowanie, podejrzane grafiki. Dziś, dzięki sztucznej inteligencji, te wiadomości są:

- napisane poprawną, naturalną polszczyzną,
- dopasowane do konkretnej osoby (np. na podstawie danych z sieci),
- spójne wizualnie z prawdziwymi stronami i markami.

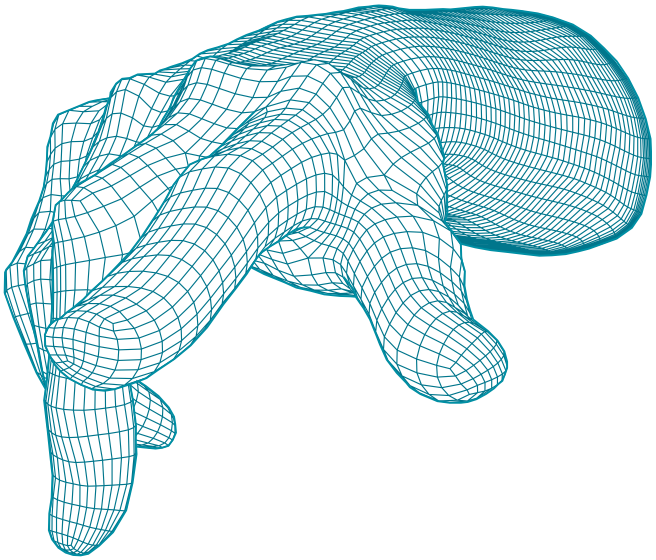
W praktyce oznacza to, że atak nie wygląda już jak oszustwo, wygląda jak coś znajomego i wiarygodnego. Sztuczna inteligencja działa tu jak przyspieszacz. To, co kiedyś wymagało czasu i umiejętności (np. napisanie przekonującej wiadomości czy przygotowanie fałszywej strony), dziś można wygenerować w kilka minut.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Ciekawostka:

Według Europejskiego Obserwatorium Mediów Cyfrowych (EDMO) skala manipulacji rośnie w zaskakującym tempie. Styczeń 2026 roku był kolejnym rekordowym miesiącem pod względem liczby fałszywych treści wygenerowanych przez AI. Aż 20% wszystkich materiałów zweryfikowanych przez ekspertów w Europie stanowiły treści stworzone lub zmanipulowane przy użyciu sztucznej inteligencji. To czwarty miesiąc z rzędu, w którym odsetek tzw. deepfake'ów i syntetycznych tekstów osiągnął rekordowy poziom.[6]

Metody socjotechniczne, czyli jak oszuści kradną Twoją tożsamość



Socjotechnika to nic innego jak psychologiczna gra. Oszuści nie szukają dziur w systemie operacyjnym – szukają dziur w Twojej czujności. Spektrum cyfrowych pułapek jest przerażająco szerokie. Podejrzane linki w wiadomościach, to pestka przy machinie psychologii kłamstwa. Od żerowania na Twojej empatii, po wykorzystanie sztucznej inteligencji, by podszyć się pod głos Twojej babci czy przyjaciela. Chyba każdy z nas ma wśród znajomych osobę, której ktoś włamał się na Messengera i wysyłał prośby o BLIKa.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Phishing, smishing i vishing – co je różni?

Phishing, smishing i vishing to formy ataków socjotechnicznych, których celem jest nakłonienie użytkowników do ujawnienia poufnych informacji. Do tego używane są fałszywe maile, strony www, wiadomości SMS, a czasem także kody QR (tzw. quishing).

Phishing – klasyczna „zarzutka". Oszust wysyła masowo wiadomości, licząc na to, że ktoś się złapie. Mają logotypy banków lub znanych firm, znajomy układ graficzny i oficjalny ton. Jeśli klikniesz i podasz dane, możesz nieświadomie dać dostęp do swojego konta lub informacji, które posłużą do dalszego oszustwa

Spear phishing – bardziej ukierunkowana wersja ataku. Oszust celuje w konkretną osobę i wcześniej zbiera o niej dostępne informacje, np. gdzie pracuje, czy i z kim współpracuje. Dzięki temu wiadomość jest znacznie trudniejsza do rozpoznania jako oszustwo

Vishing – phishing przez telefon. Oszust dzwoni, podszywając się np. pod pracownika banku lub policjanta. Wykorzystuje presję czasu i emocje, próbując wyłudzić dane, kody (np. BLIK) albo nakłonić do wykonania przelewu.

Smishing – phishing w wiadomościach SMS. Krótkie komunikaty typu „Twoja paczka została wstrzymana" czy „Twoje hasło wygasa" zawierają link prowadzący do fałszywej strony, która ma na celu wyłudzenie danych.

Złota zasada: Jeśli wiadomość wymusza na Tobie pośpiech i obiecuje nagrodę lub grozi konsekwencjami – zatrzymaj się. Nigdy nie klikaj w linki do płatności przesyłane w SMS-ach, e-mailach. Nie podawaj swoich danych w pośpiechu, nie wypełniaj formularzy, wymuszających szybkie działania. Lepiej wejdź na oficjalną stronę lub aplikację banku/firmy/kuriera i sprawdź samodzielnie, czy czeka na Ciebie jakiś komunikat.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Bezpieczeństwo konta: dlaczego 2FA to absolutne minimum?

Masz jedno, „trudne" hasło do wszystkiego? No to jesteś ulubionym typem celu dla hakerów. Wystarczy jeden wyciek danych z małego sklepu internetowego, w którym kupiłeś koszulkę albo kosmetyki 3 lata temu, a Twoje hasło trafia na czarny rynek.

Wtedy jedyną rzeczą, która stoi między hakerem a Twoimi zdjęciami, e-mailami i pieniędzmi, jest 2FA (z ang. Two-Factor Authentication), czyli uwierzytelnianie dwuskładnikowe.

Dlaczego hasło to za mało? Hasła są kradzione codziennie. Jeśli używasz tego samego hasła na Instagramie i do maila, haker ma komplet i naprawdę nie musi się natrudzić, by dostać się do Twojego cyfrowego życia.

Jak działa 2FA? To dodatkowa warstwa ochrony. Nawet jeśli ktoś pozna Twoje hasło, system zapyta o drugi składnik: kod z SMS-a, powiadomienie w aplikacji (np. Google Authenticator) lub fizyczny klucz bezpieczeństwa.

To jak drugi zamek w drzwiach. Złodziej może mieć klucz do pierwszego zamka (hasło), ale bez tego drugiego (kodu z Twojego telefonu) i tak nie wejdzie do środka.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

KRAJOWY PLAN ODBUDOWY

Rzeczpospolita Polska

Sfinansowane przez Unię Europejską NextGenerationEU

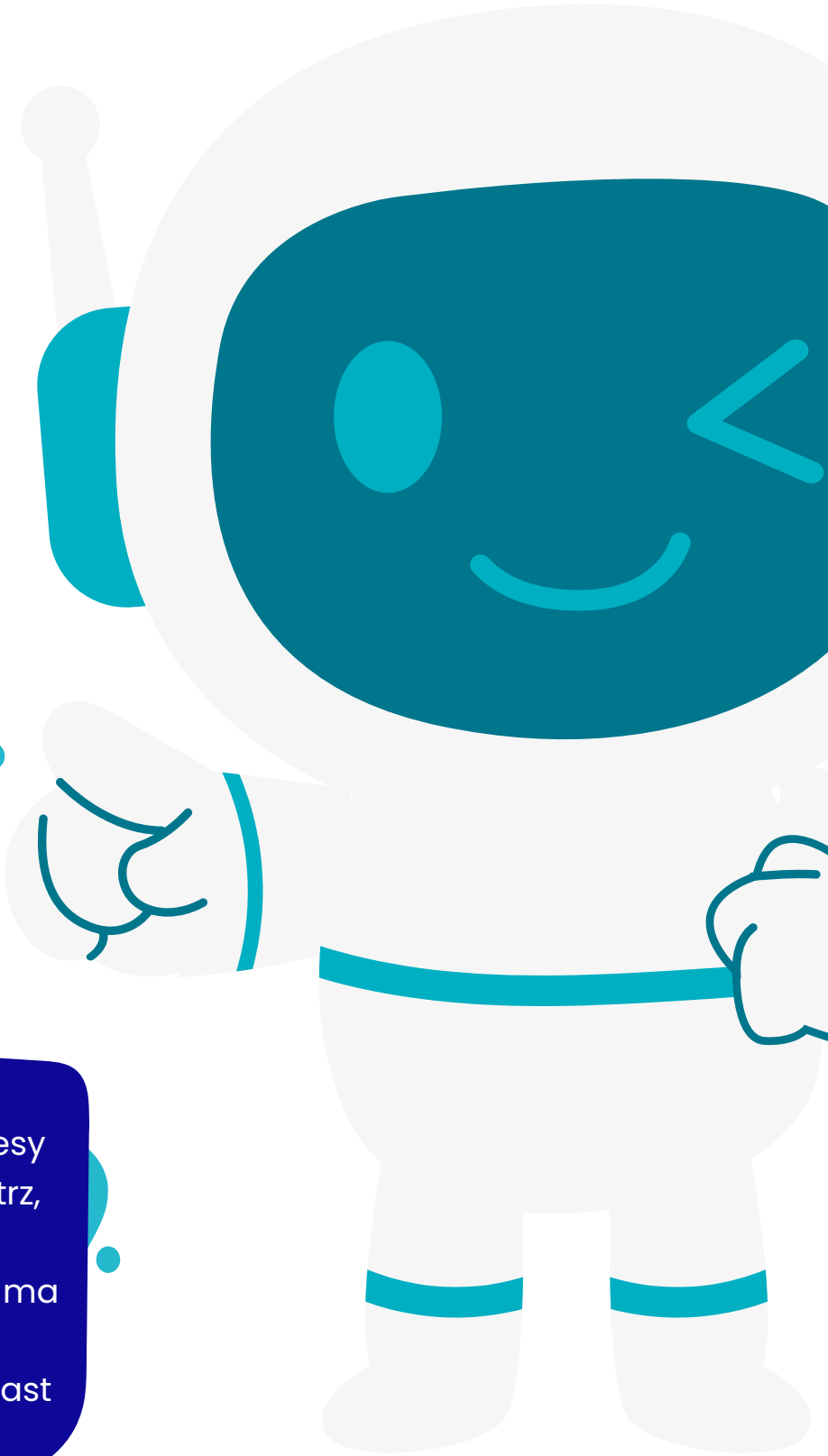
WOJEWÓDZTWO POMORSKIE

Twoja paranoja to najlepsza polisa ubezpieczeniowa.

Zmień to od razu:

1.

Włącz 2FA na każdym koncie, na którym Ci zależy (social media, e-mail, bank, skrzynka e-mailowa).



2.

Używaj menedżera haseł. Nie musisz pamiętać 50 skomplikowanych ciągów znaków. Niech program robi to za Ciebie.

3.

Sprawdzaj adresy URL. Zawsze patrz, czy w pasku przeglądarki nie ma literówki (np. mbanke.pl zamiast mbank.pl).

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

POMORSKIE KOMPETENCJE JUTRA

FUNDACJA NIE WIDAĆ PO MNIE

Wsparcie psychologiczne – kiedy ataki lub dezinformacja uderzają w zdrowie psychiczne

Współczesne ataki w sieci i zalew dezinformacji nie uderzają wyłącznie w Twoje samopoczucie „tu i teraz". Ich konsekwencje są wielowymiarowe i rozłożone w czasie, a wszystko zaczyna się w Twoim mózgu. Czy wiesz, że Twój umysł nie rozróżnia ataku słownego na ekranie od fizycznego zagrożenia w realu? W obu przypadkach reaguje tak samo: wyrzutem kortyzolu, przyspieszonym tętnem i wejściem w tryb „podejmij działanie lub nie". Problem polega na tym, że przed hejtem w sieci trudno uciec. To sprawia, że Twój mózg przechodzi w stan ciągłego czuwania. Pojawia się dezorientacja i zmęczenie, przez które trudniej Ci się uczyć, skupić na pasji czy podjąć nawet proste decyzje.[7]

Mechanizm oszustwa, czyli efekt iluzorycznej prawdy

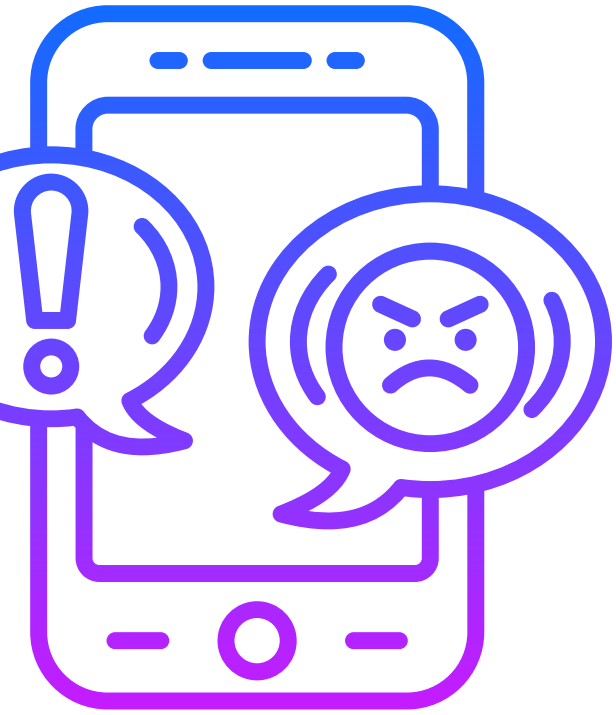
Dezinformacja wykorzystuje tę lukę w Twoim systemie obronnym, stosując tzw. efekt iluzorycznej prawdy (z ang. illusory truth effect). Opiera się on na łatwości poznawczej. Kiedy czytasz fake newsa po raz pierwszy, Twój krytyczny umysł mówi: „To bzdura". Jednak, gdy ten sam kłamliwy nagłówek mignie Ci na TikToku, w memie na Instagramie, a potem powtórzy go ktoś znajomy, mózg zaczyna go rozpoznawać. Ta znajomość komunikatu jest przez naszą podświadomość błędnie interpretowana jako wiarygodność. Mózg idzie na skróty – skoro to skądś znam, to pewnie coś w tym jest.

Najgorsze jest to, że ten mechanizm działa nawet wtedy, gdy wiesz, że dana informacja jest nielogiczna. Samo się z nią „osłuchanie" buduje w Tobie dziwny rodzaj zaufania. Trolle i boty nie muszą Cię przekonywać mądrymi argumentami – wystarczy, że zaleją Twoją przestrzeń tym samym kłamstwem tyle razy, aż uznasz je za element rzeczywistości. W efekcie zaczynasz działać w oparciu o iluzję. Unikasz pewnych ludzi lub rezygnujesz z aktywności, bo „wszyscy o tym mówią". Dlatego dziś umiejętność krytycznego myślenia to Twoja najważniejsza kompetencja cyfrowa.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Skala problemu: nie jesteś w tym sam(a)

To, że dezinformacja i ataki stały się częścią naszej codzienności, nie oznacza, że musisz się na nie godzić. Dane z raportu Nastolatki 3.0[2] pokazują, jak ogromna jest skala tego zjawiska:



Co trzeci z Twoich znajomych był w sieci wyzywany lub poniżany.

68% nastolatków uważa, że mowa nienawiści to w Polsce ogromny problem.

Prawie połowa młodych ludzi (47%), którzy doświadczyli agresji w sieci, nie zrobiła z tym kompletnie nic.

Blisko 40% ofiar przemocy internetowej nie zgłasza problemu, nie szuka pomocy, nie informuje o zdarzeniu. Nie jesteś jedyną osobą, która zamarła, czytając hejt. Prawie co drugi z Twoich rówieśników czuje taką samą blokadę. Ale to milczenie to paliwo dla hejtera. Czas to zmienić.

To, że dezinformacja i ataki stały się częścią naszej internetowej rzeczywistości, wcale nie oznacza, że musisz się godzić na jej zasięg. Nie myl odpuszczania (ignorowanie dla własnego świętego spokoju) z poddawaniem się.

Dlaczego to boli (i dlaczego to normalne)?

Dezinformacja może uderzać w Twoje najbardziej podstawowe potrzeby: bezpieczeństwo i przynależność.

Pamiętaj, hejt to nie jest opinia. Opinia może brzmieć: „Nie podoba mi się Twoja bluza". Hejt ma inny wymiar: „Jesteś beznadziejny, bo nosisz tę bluzę". Ma na celu nieakceptowalny atak na Twoją tożsamość.

Efekt skali oddziałowuje na Ciebie mocniej. W świecie offline słyszysz obelgę raz. W sieci widzisz ją podświetloną, polajkowaną i udostępnioną. Twój mózg interpretuje to napiętnowanie w pewnej przestrzeni publicznej – a to może generować w Tobie lęk.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

– Hejt i dezinformacja to nie są opinie, z którymi musisz dyskutować. To cyfrowe toksyny. Twój mózg reaguje na nie tak samo, jak na fizyczne zagrożenie, dlatego masz prawo czuć lęk, złość czy bezsilność. Pamiętaj, że dbanie o swoje granice w sieci to nie przejaw słabości, ale najwyższa forma samoobsługi psychicznej. Jeśli czujesz, iż masz dość tych emocji – nie duś ich w sobie. To, czego nie widać na zewnątrz, potrafi najmocniej ciążyć w środku. – *wyjaśnia psycholog Agnieszka z Fundacji Nie Widać Po Mnie.*

To, że dezinformacja i ataki stały się częścią naszej codzienności, nie oznacza, że musisz się na nie godzić. Dane z raportu Nastolatki 3.0[2] pokazują, jak ogromna jest skala tego zjawiska:

Gdzie szukać pomocy?

Telefon Zaufania dla dzieci i młodzieży **116-111**. Dyżurują w nim konsultanci (psycholodzy, pedagodzy), z którymi można podzielić się swoimi trudnościami, otrzymać wsparcie i porady, które pomogą radzić sobie w trudnych sytuacjach. Możesz porozmawiać o wszystkim. Telefon czynny jest codziennie przez całą dobę.

Działaniu telefonu towarzyszy strona internetowa **www.116111.pl**, która umożliwia zadawanie anonimowych pytań on-line przez całą dobę – poszukaj ikonki.

Możesz porozmawiać o wszystkim - także wtedy, gdy coś po prostu Cię martwi albo czujesz się niepewnie, np. w sieci. Nikt nie będzie Cię oceniał.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Twoje cyfrowe BHP

Pamiętaj, że bezpieczeństwo w sieci nie sprowadza się zaledwie do zmiany hasła na trudniejsze. To przede wszystkim Twoja odporność na manipulację, hejt i zmęczenie informacyjne. Czas na szybki audyt Twojej cyfrowej twierdzy.

– Twoja pewność siebie w sieci paradoksalnie bierze się z tego, co masz poza nią: z autentycznych relacji z ludźmi, którym ufasz. Gdy w necie robi się toksycznie, Twoim realnym wsparciem mogą być rówieśnicy, rodzina, najbliżsi. – dodaje psycholog Agnieszka.

Nie daj sobie wmówić, że dezinformacja to nie Twój problem. To, że rzadko reagujemy na fejki, często wynika z poczucia, że i tak nic nie zmienimy. Ale prawda jest taka, że każdy Twój świadomy wybór – to, co podasz dalej, a co zablokujesz – realnie kształtuje świat, w którym żyjemy. Bądź tym, który wie, jak grać w tę grę na własnych zasadach. **– podsumowuje.**

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Krótki quiz bezpieczeństwa: Czy jesteś bezpieczny/bezpieczna w sieci?

Przy każdym punkcie zaznacz: TAK, NIE lub CZASEM. Bądź ze sobą szczery – nikt tego nie ocenia poza Tobą.

Czy masz włączone uwierzytelnianie dwuskładnikowe (2FA) na Instagramie, TikToku i mailu? (To ten kod SMS lub w apce, który wpisujesz po haśle).

☐ Tak ☐ Nie ☐ Czasami

Czy zdarzyło Ci się udostępnić newsa, czytając jego krzykliwy nagłówek, bez klikania w środek?

☐ Tak ☐ Nie ☐ Czasami

Czy blokujesz profile, które regularnie psują Ci humor lub zalewają Cię agresją, zamiast z nimi dyskutować?

☐ Tak ☐ Nie ☐ Czasami

Czy potrafisz rozpoznać deepfake? (Zwracasz uwagę na nienaturalne mruganie oczu, dziwny dźwięk głosu lub rozmazane krawędzie twarzy na filmie?).

☐ Tak ☐ Nie ☐ Czasami

Czy odkładasz telefon w innym pokoju lub ustawiasz w trybie „uśpienia” na minimum 30 minut przed snem?

☐ Tak ☐ Nie ☐ Czasami

Czy sprawdzasz źródło informacji, zanim uznasz ją za prawdziwą? (np. czy profil na X ma historię, czy powstał tydzień temu?).

☐ Tak ☐ Nie ☐ Czasami

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych” jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Wyniki

Większość TAK: jesteś cyfrowym ninją. Twoja świadomość jest na dość wysokim poziomie, a manipulatorzy nie mają z Tobą lekko

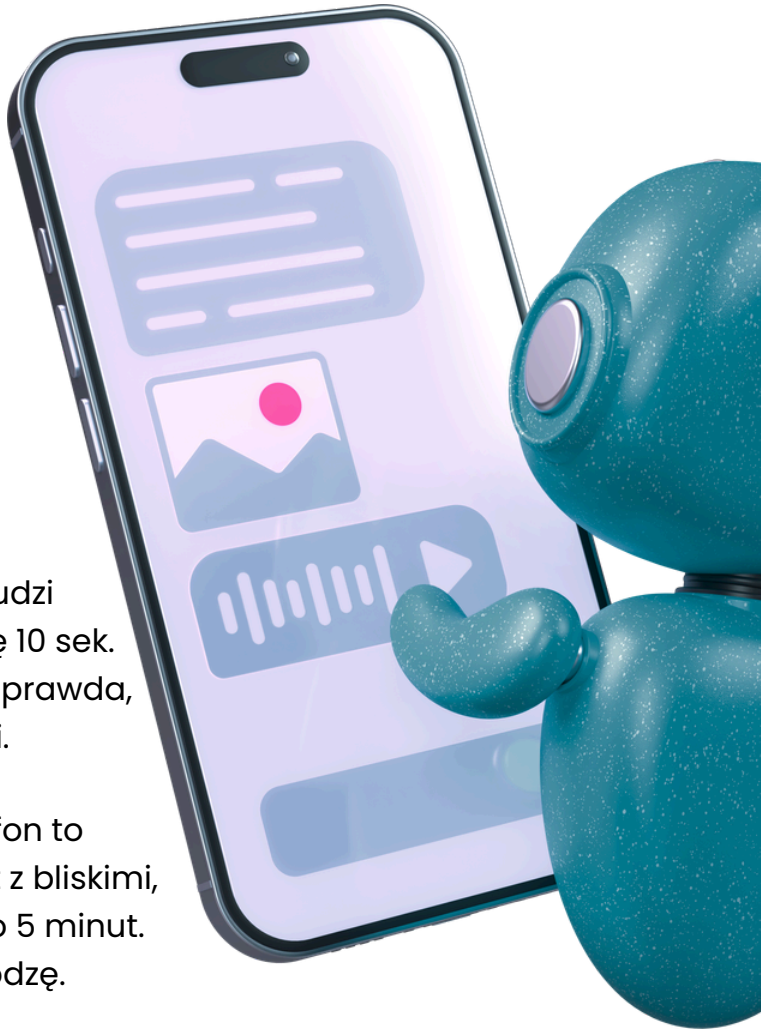
Większość CZASEM: zdarzają Ci się pęknięcia, ale możesz je łatwo naprawić.

Większość NIE: Twój cyfrowy dom ma otwarte drzwi i okna. Czas wziąć sprawy w swoje ręce, zanim ktoś (lub coś) wejdzie Ci na głowę.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Manifest świadomego użytkownika

Skoro już wiesz, jak działają mechanizmy przyciągania Twojej uwagi, czas na działanie, a właściwie na kontratak. Postarajmy się wspólnie stworzyć kodeks cyfrowej wolności. Bycie świadomym użytkownikiem to dzisiaj najwyższa forma buntu przeciwko manipulacji.



Kilka zasad cyfrowej odporności:

Moja uwaga to mój najcenniejszy zasób. Nie oddaję jej za darmo każdemu, kto użyje krzykliwego nagłówka lub czarno-białego zdjęcia. Wybieram, co oglądam, zamiast pozwalać, by algorytm wybierał za mnie. Zaznaczam, że to mnie nie interesuje, blokuję spam i świadomie stawiam granice.

Weryfikuję, zanim poczuję. Kiedy treść budzi we mnie nagły gniew, lęk lub euforię, robię 10 sek. przerwy. Tak sprawdzam czy to może być prawda, czy tylko próba zhakowania moich emocji.

Rozróżniam narzędzie od pułapki. Smartfon to moje okno na świat, baza wiedzy i kontakt z bliskimi, a nie smycz, która ściąga mnie do sieci co 5 minut. Ja decyduję, kiedy wchodzę i kiedy wychodzę.

Szanuję swój czas (i swój sen). Algorytmy nie śpią, ale ja muszę. Moje życie w realu, w tym spotkania, sport, pasje – ma pierwszeństwo przed nieskończonym scrollowaniem. Dlatego mój telefon nie śpi ze mną w łóżku, nie jest non stop w zasięgu mojej ręki.

Nie daję się nabrać na perfekcję. Wiem, że 90% tego, co widzę, przeszło przez filtry, AI lub sztab specjalistów od wizerunku. Moja wartość nie zależy od porównywania się do cyfrowych iluzji.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Jestem strażnikiem własnej prywatności. Moje dane to moja historia. Nie rozdaję ich każdemu formularzowi w Internecie i dbam o to, co o sobie publikuję. Uważam z jakimi sieciami łączę się w wakacje, poza domem. Zanim podam znajomemu szybkiego BLIKa, dzwonię zapytać, czy naprawdę go potrzebuje. Uczę też moich najbliższych, by dbali o swoje cyfrowe bezpieczeństwo.

Reaguję, gdy widzę syf. Nie jestem biernym widzem. Kiedy widzę dezinformację, hejt lub patostreamy, nie daję im zasięgu – po prostu zgłaszam i blokuję. Moja cisza to moja siła.

Dodaj też swoje zasady:

.....

.....

.....

Teraz Twój ruch, by ten manifest nie był wyłącznie teorią. Dodaj do niego własne punkty. Określ, jak chcesz dbać o swoje cyfrowe bezpieczeństwo i komfort. Wydrukuj go sobie albo zrób screena, zaglądaj do niego i na bieżąco odświeżaj.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Cyfrowa apteczka: gdzie zgłaszać oszustwa i ataki cyfrowe?

Wiedza o tym, jak się bronić, to połowa sukcesu. Druga połowa to wiedza, gdzie uderzyć, gdy ktoś próbuje Cię oszukać, okraść lub zastraszyć. W Polsce mamy od tego wyspecjalizowane jednostki, które reagują szybciej, niż myślisz. Zanim do nich przejdziemy, zostawiamy Ci ważne przypomnienie od psycholożki Fundacji Nie Widać Po Mnie, Agnieszki:

Często myślimy, że przyznanie się do bycia ofiarą hejtu, oszustwa to słabość, albo że sami sobie z tym poradzimy. To pułapka. Kiedy ktoś Cię atakuje w sieci, Twoje poczucie bezpieczeństwa zostaje naruszone, a emocje, które się pojawiają mogą być zbyt ciężkie, by nosić je w pojedynkę. Powiedzenie o tym zaufanej osobie: rodzicowi, przyjacielowi czy nauczycielowi – to nie jest skarżenie się.

Twoi bliscy często nie mają pojęcia, co dzieje się w Twojej sieci, nie dlatego, że ich to nie obchodzi, ale dlatego, że milczymy. Dając im znać, budujesz wokół siebie bezpieczną strefę. Pamiętaj, że obecność drugiej osoby obok Ciebie drastycznie obniża poziom stresu w Twoim organizmie. Razem łatwiej jest odróżnić kłamstwo od prawdy i podjąć konkretne kroki prawne czy techniczne. Wsparcie to Twoje najsilniejsze narzędzie.

CERT Polska (Computer Emergency Response Team) to zespół ekspertów, którzy pilnują bezpieczeństwa polskiego Internetu. Widzisz podejrzany sklep, chcesz zgłosić domenę internetową służącą do wyłudzeń danych i środków finansowych? Dostałeś dziwnego SMS-a z linkiem do dopłaty za paczkę? Nie kasuj go od razu, tylko zgłoś.

- Formularz online na stronie **incydent.cert.pl**.
- SMS: Prześlij podejrzaną wiadomość na numer 8080.
- E-mail: Wyślij wiadomość na cert@cert.pl.
- Zgłoszenie telefoniczne w przypadku pilnych incydentów (tel. 22 380 83 99).

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Dyżurnet.pl (NASK). Jeśli trafisz w sieci na treści, które są nielegalne (np. materiały przedstawiające wykorzystywanie dzieci) lub spotkasz się z ekstremalną formą cyberprzemocy, zgłoś to do Dyżurnet.pl. To punkt kontaktowy działający w strukturach NASK.

- Przez formularz na stronie, mailowo na adres: dyzurnet@dyzurnet.pl lub przez aplikację mobilną.
- Co zgłaszać? Wszystko, co budzi Twój niepokój i wydaje się łamać prawo – od hejtu, przez patostreamy, po nielegalne materiały wideo.

Aplikacja mObywatel. Dzięki aktualizacji 2.0. każdy korzystający z najnowszej wersji będzie mógł jeszcze szybciej zgłosić oszustwo w Internecie.

Demagog - na stronie https://demagog.org.pl/zglos-do-weryfikacji/ możesz zgłosić fake newsa albo fałszywą wypowiedź osoby publicznej.

Policja i prokuratura

Jeśli padłeś ofiarą przestępstwa – ktoś ukradł Ci pieniądze z konta, szantażuje Cię Twoimi prywatnymi zdjęciami (sextortion) lub włamał się na Twoje profile i przejął Twoje dane – samo zgłoszenie do CERT nie wystarczy. Musisz udać się na najbliższą jednostkę policji.

- Możliwe jest również złożenie zawiadomienia za pomocą https://www.gov.pl/web/gov/zglos-przestepstwo.
- Zabezpiecz dowody! Zrób screenshoty rozmów, komentarzy, zachowaj potwierdzenia przelewów i linki do fałszywych stron. To Twoja broń w procesie odzyskiwania sprawiedliwości.

Zgłaszając oszustwo w każdej postaci dbasz o swój dobrostan psychiczny, ale i zapobiegasz rozprzestrzenianiu się takich ataków albo dezinformacji dalej.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

Bibliografia

[1] Digital economy and society statistics - households and individuals, Eurostat, Eurostat - Internet use by individuals, dostęp na dzień 3 marca 2026 r.;

[2] Raport "Nastolatki 3.0" (edycja 2024), NASK;

[3] Inside the funhouse mirror factory: How social media distorts perceptions of norms, Robertson, C. E., del Rosario, K. S., Van Bavel, J. J.;

[4] Evaluating Information: The Cornerstone of Civic Online Reasoning, Stanford History Education Group (SHEG), Stanford - Civic Online Reasoning Report;

[5] Raport "Social Media 2025", Mediapanel Gemius/PBI;

[6] Europejskie Obserwatorium Mediów Cyfrowych (EDMO) oraz raporty Europolu dotyczące przyszłości przestępczości i treści syntetycznych;

[7] Wyloguj swój mózg, Anders Hansen;

[8] Portal i poradniki Cyberprofilaktyka NASK, dostęp na dzień 3 marca 2026;

[9] Krajobraz bezpieczeństwa polskiego internetu (2024/2025), roczny raport, CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2024.pdf, dostęp na dzień 3 marca 2026;

[10] Demagog.org.pl – sekcja „Edukacja", dostęp na dzień 3 marca 2026;

[11] Tackling Online Disinformation, Oficjalne wytyczne UE dotyczące walki z dezinformacją i regulacji platform (DSA), European Commission, ec.europa.eu, dostęp na dzień 1 marca 2026;

[12] Better Internet for Kids (BIK), Europejska sieć promująca bezpieczny internet, betterinternetforkids.eu, dostęp na dzień 3 marca 2026;

[13] American Psychological Association https://www.apa.org/topics/social-media-internet/youth-social-media-2024, dostęp na dzień 3 marca 2026.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

O autorze

Kamila Dąbrowska

Z wykształcenia prawniczka i mediatorka, jednak to komunikacji medycznej oddała serce i ostatnie 20 lat swojego zawodowego życia. Przez lata zarządzała dużymi projektami medialnymi, współpracując z największymi dziennikami w Polsce, takimi jak „Gazeta Wyborcza" czy „Rzeczpospolita".

Swoją energię i wiedzę angażuje w projekty, które realnie zmieniają codzienność – od pracy w redakcjach portali medycznych, przez wspieranie organizacji NGO, aż po komunikację w placówkach rehabilitacyjnych. Swoje miejsce odnalazła w działalności Fundacji Nie Widać Po Mnie.

Wierzy, że każda chwila poświęcona na realną pomoc drugiemu człowiekowi to najważniejsza inwestycja w świat, w którym dobro i empatia są po prostu standardem. Dla niej edukacja zdrowotna to nie tylko suche fakty, ale klucz do tego, byśmy wszyscy czuli się lepiej – we własnym ciele i we własnej głowie. Zamiast skomplikowanych definicji wybiera praktyczne rozwiązania, które pomagają oswoić trudne tematy.

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.

O Fundacji Nie Widać Po Mnie

Fundacja Nie Widać Po Mnie zrodziła się z potrzeby przełamywania tabu i głośnego mówienia o zdrowiu psychicznym Polaków i problemach, takich jak depresja, uzależnienia, lęki i fobie. Wierzymy, że odpowiednia psychoedukacja i zwiększanie świadomości jest istotnym elementem profilaktyki zdrowotnej, która pozwoli w przyszłości zmniejszyć ryzyko zaburzeń psychicznych i zahamuje tendencję wzrostową zapadalności na tego typu choroby, których konsekwencje odczuwają pacjenci, rodzina i cały system opieki zdrowotnej.

Swoje działania kierujemy do różnych grup wiekowych oraz zawodowych. Odkrywamy czynniki zwiększające prawdo-podobieństwo zaburzeń, a także uczymy, jak to zagrożenie zmniejszać. Realizujemy programy psychologicznej pomocy dla osób dorosłych w kryzysie. Troszczymy się też o seniorów.

Troską otaczamy też dzieci i młodzież. Wirtualna rzeczywistość, deprecjonowanie życia „w realu", samotność, rosnąca depresja, uzależnienia od substancji i czynności, cyberprzemoc — to tylko kilka z listy problemów, które piętrzą się dziś przed młodymi ludźmi.

Programy psychoedukacyjne kierujemy też do medyków, którzy w sposób szczególny zagrożeni są zaburzeniami typu depresja, uzależnienia, lęki, zespół stresu pourazowego czy wypalenie zawodowe. Wierzymy, że odczarowanie heroizmu w zawodach ochrony zdrowia pozwoli wielu medykom przełamać strach przed właściwą terapią, a to wpłynie na jakość usług i poprawi funkcjonowanie całego systemu.

Więcej informacji o naszych programach i podejmowanych działaniach dostępnych jest na naszej stronie internetowej www.niewidacpomnie.org

Projekt „Zbudowanie systemu koordynacji i monitorowania regionalnych działań na rzecz kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie, w tym uczenia się dorosłych" jest finansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności.