KRAJOWY PLAN ODBUDOWY

Rzeczpospolita Polska

Sfinansowane przez Unię Europejską NextGenerationEU

WŁĄCZAMY CYFROWO Mazowsze SZKOLENIA DLA OSÓB W WIEKU 55+

CYBER-BEZPIECZEŃSTWO I FAKE NEWSY

PIGUŁKA WIEDZY

Pro Cultura WŁĄCZAMY CYFROWO

AgeHUB FUNDACJA

Kreatywni 50+

FUNDACJA PARTYCYPACJI SPOŁECZNEJ

FUNDACJA REGENERACJA

ZACZYN FUNDACJA

Autor: Łukasz Szczepańczyk

Opracowanie graficzne: Małgorzata Szlendak

Publikacja powstała w ramach projektu: „Włączamy Cyfrowo Mazowsze – szkolenia dla osób w wieku 55 plus” realizowanego w ramach Inwestycji C2.1.3 „E-kompetencje” Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), finansowanego ze środków Unii Europejskiej w ramach instrumentu NextGenerationEU.

Publikacja dostępna jest bezpłatnie na stronie www.wlaczamycyfrowo.pl

Materiał ukończono: październik 2025 r.

ZAKRES KURSU

Moduł 1 – Fake newsy, clickbaity i manipulacje w przestrzeni publicznej (3,5 godz.)

- Rozpoznawanie fałszywych informacji w Internecie i mediach społecznościowych.
- Poznanie metod weryfikacji informacji: sprawdzanie źródła, autora i daty publikacji.

Moduł 2 – Dezinformacja i oszustwa w przestrzeni prywatnej (3,5 godz.)

- Zrozumienie zjawiska phishingu, smishingu, vishingu i spoofingu.
- Analiza zagrożeń w komunikatorach, mediach społecznościowych i na portalach ogłoszeniowych.

Moduł 3 – Cyberbezpieczeństwo i higiena cyfrowa (3,5 godz.)

- Bezpieczeństwo danych osobowych i prywatności w sieci: co można, a czego nie należy udostępniać.
- Ochrona finansów online: fałszywe płatności, formularze, bankowość i serwisy sprzedażowe.
- Zabezpieczanie sprzętu: aktualizacje, programy antywirusowe, zapora sieciowa i kopie zapasowe.

Moduł 4 – Sztuczna inteligencja: możliwości, zagrożenia i weryfikacja treści (3,5 godz.)

- Zrozumienie, czym jest sztuczna inteligencja i jak działa w codziennym życiu.
- Rozpoznawanie treści generowanych przez AI: zdjęcia, głosy, deepfake, fałszywe paski informacyjne.

Słowniczek

1. **Fake news** – fałszywa lub zmanipulowana informacja, mająca wzbudzić emocje lub wprowadzić odbiorcę w błąd.
2. **Dezinformacja** – celowe rozpowszechnianie nieprawdziwych wiadomości, aby wpływać na opinię publiczną.
3. **Clickbait** – chwytliwy tytuł lub obraz, który ma zachęcić do kliknięcia w artykuł, często kosztem prawdziwości treści.
4. **Phishing** – próba wyłudzenia danych osobowych lub finansowych przez fałszywe e-maile, SMS-y lub strony internetowe.
5. **Smishing** – odmiana phishingu prowadzona przez wiadomości SMS, np. o rzekomej paczce lub dopłacie.
6. **Vishing** – oszustwo telefoniczne, w którym ktoś podszywa się pod bank lub urzędnika, by wyłudzić dane.
7. **Spoofing** – podszywanie się pod inną osobę lub instytucję, np. przez numer telefonu lub adres e-mail.
8. **Deepfake** – fałszywe nagranie wideo lub audio stworzone przez sztuczną inteligencję, które wygląda jak prawdziwe.
9. **Algorytm** – zestaw instrukcji, według których komputer lub aplikacja analizuje dane i podejmuje decyzje.
10. **Bańka informacyjna** – sytuacja, w której widzimy w Internecie tylko treści zgodne z naszymi poglądami.
11. **Bot** – program automatycznie publikujący lub komentujący treści w sieci, często wykorzystywany do manipulacji.
12. **Fact-checking** – sprawdzanie prawdziwości informacji przez specjalne serwisy, np. *Demagog.pl* lub *Fakenews.pl*.
13. **Higiena cyfrowa** – zestaw zasad bezpiecznego korzystania z technologii, np. silne hasła i przerwy od ekranu.

14. **Uwierzytelnianie dwuskładnikowe (2FA)** – dodatkowe potwierdzenie logowania, np. kodem SMS lub aplikacją bankową.
15. **Ransomware** – złośliwe oprogramowanie, które blokuje dostęp do danych i żąda okupu za ich odblokowanie.
16. **Hasło zdaniowe** – długie hasło w formie łatwego do zapamiętania zdania, np. *MojaKawaTo3Filiżanki!*.
17. **Oszustwo inwestycyjne** – fałszywa oferta szybkiego zarobku, np. w kryptowaluty lub akcje, często z użyciem wizerunku znanych osób.
18. **Podszywanie się (impersonacja)** – tworzenie fałszywego profilu lub konta, by udawać kogoś innego.
19. **Wyszukiwanie wsteczne** – metoda sprawdzania pochodzenia zdjęcia lub filmu poprzez wyszukiwarkę (np. Google Obiektyw).
20. **CERT Polska** – zespół ekspertów, do którego można zgłaszać próby oszustwa, phishingu i inne zagrożenia w sieci.

Własne, ważne i nowe pojęcia

_____

_____

_____

_____

_____

_____

_____

Moduł 1: Dezinformacja, fake newsy i zagrożenia w cyfrowej przestrzeni publicznej

Co to jest fake news i po czym można go rozpoznać ?

Fake news to fałszywa lub zmanipulowana informacja, która ma wzbudzić silne emocje, przyciągnąć uwagę lub przekonać odbiorcę do określonego poglądu. Czasem jest tworzony celowo – aby zaszkodzić komuś lub wywołać zamieszanie. Innym razem powstaje przez przypadek, gdy ktoś nieświadomie udostępnia nieprawdziwą wiadomość.

Fake news może dotyczyć wszystkiego:

- zdrowia (np. „czosnek leczy raka”),
- wydarzeń społecznych (np. „w Polsce zamykają wszystkie szkoły”),
- polityki, pogody, a nawet znanych osób.

Najczęściej rozprzestrzenia się w mediach społecznościowych, na portalach informacyjnych i w komunikatorach, gdzie ludzie udostępniają treści bez ich wcześniejszego sprawdzenia.

Po czym można poznać fake news?

1. **Brak autora lub źródła** – artykuł lub post nie ma podpisu, a strona nie podaje, kto jest jej właścicielem.
2. **Brak daty publikacji** – informacja może być stara, ale przedstawiana jest jako aktualna.
3. **Emocjonalny ton** – tekst wzbudza silne uczucia: złość, lęk, oburzenie lub zachwyt.

4. **Użycie przesadzonych słów** – „szokujące”, „nikt o tym nie mówi”, „ukrywana prawda”, „natychmiast udostępnij”.
5. **Błędy językowe i literówki** – często świadczą o szybkim, nieprofesjonalnym przygotowaniu treści.
6. **Brak potwierdzenia w innych źródłach** – po wpisaniu hasła w wyszukiwarce okazuje się, że żadne znane media o tym nie piszą.
7. **Zmanipulowane zdjęcia lub filmy** – po wyszukaniu obrazu w Google Obiektyw widać, że pochodzi z innego wydarzenia lub kraju.

Jak się bronić przed fake newsami

- **Zatrzymaj się przed udostępnieniem** – przeczytaj jeszcze raz i zadaj sobie pytanie: „czy to naprawdę ma sens?”.
- **Sprawdź źródło** – wpisz tytuł w wyszukiwarce i zobacz, czy inne media o tym mówią.
- **Korzystaj z serwisów sprawdzających fakty**, takich jak Demagog.org.pl czy Fakenews.pl.
- **Nie udostępniaj emocjonalnych postów od nieznanych osób** – nawet jeśli wydają się „prawdziwe”.

Twoje notatki:

_____

_____

_____

_____

_____

Ćwiczenie: rozpoznawanie fake news'ów

Zaznacz elementy z poniższego postu, które mogą sugerować, że jest to fake news?

„Rząd planuje wyłączyć Internet w całym kraju na trzy dni – przecieki z tajnego dokumentu!"

TREŚĆ POSTA:

Jak informuje anonimowe źródło z kręgów rządowych, już w przyszłym tygodniu planowane jest ***czasowe odłączenie Internetu w Polsce****.*

Decyzja ma być częścią „akcji bezpieczeństwa cyfrowego" i testem gotowości na cyberatak.

Według nieoficjalnych informacji ***sieć ma zostać wyłączona na 72 godziny****, a dostęp będą mieć tylko wybrane instytucje państwowe.*

Eksperci ostrzegają, że ***może dojść do chaosu w bankach i sklepach internetowych****.*

Niektóre serwisy już teraz przygotowują się do pracy offline.

„Nikt nie mówi o tym głośno, ale mamy potwierdzenie z trzech niezależnych źródeł" *– twierdzi redakcja portalu Nowe Info24.*

Podziel się tą informacją ze znajomymi, ***zanim będzie za późno!***

Elementy świadczące o nieprawdziwości informacji:

_____

_____

_____

_____

_____

_____

Co to jest clickbait i jak go rozpoznać?

Clickbait to chwytliwy **tytuł, nagłówek lub obraz**, którego głównym celem jest **nakłonienie użytkownika do kliknięcia w link** – niezależnie od tego, czy treść jest prawdziwa lub wartościowa.

Słowo „clickbait" pochodzi od angielskich słów *click* (kliknięcie) i *bait* (przynęta). To właśnie **„przynęta na kliknięcia"** – sposób, w jaki portale zdobywają odsłony, a tym samym zarabiają na reklamach.

Clickbait często obiecuje sensację, szok albo „tajemnicę", ale po kliknięciu okazuje się, że artykuł nie zawiera niczego nowego, ważnego ani prawdziwego.

Po czym można rozpoznać clickbait?

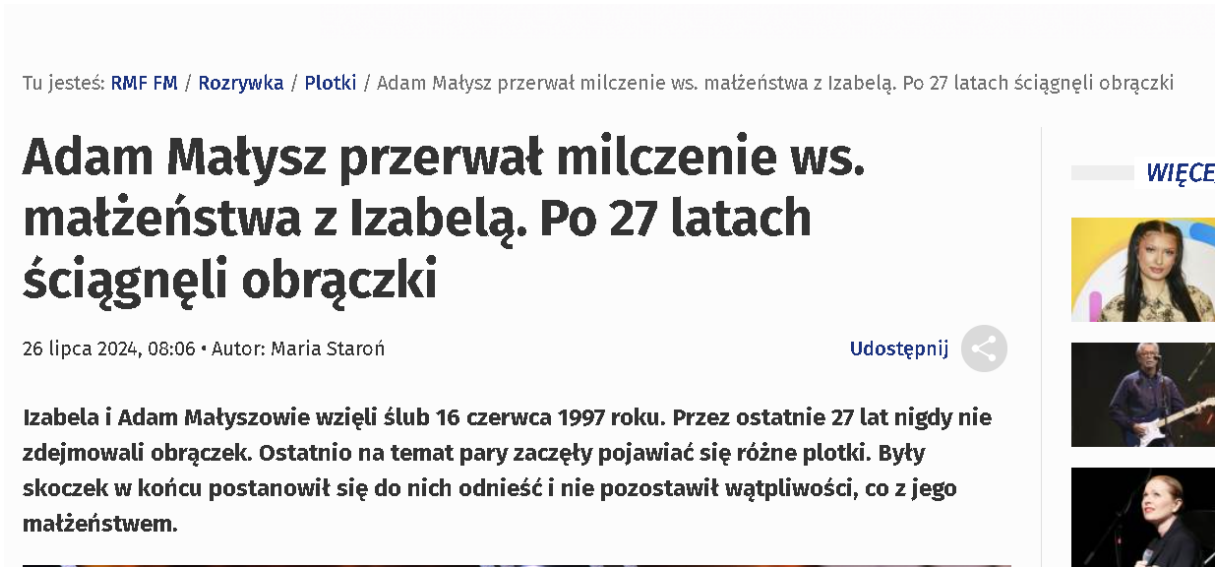
1. **Przesadzone lub emocjonalne tytuły** – np. „Nie uwierzysz, co wydarzyło się po tym, gdy zjadła banana!", „Ten trik lekarzy zmieni twoje życie!".
2. **Słowa wywołujące ciekawość lub lęk** – „szokujące", „niesamowite", „tajemnicze", „natychmiast", „ukrywane przez rząd".
3. **Brak konkretów** – tytuł obiecuje coś niezwykłego, ale nie podaje żadnych faktów.
4. **Fałszywa obietnica** – po wejściu na stronę okazuje się, że treść nie ma nic wspólnego z tytułem.
5. **Wiele reklam i pop-upów** – artykuł jest pretekstem, żeby użytkownik zobaczył reklamy, a nie dostał informacji.

Ćwiczenie: rozpoznawanie clickbait'ów

Na załączonych zrzutach ekranu podkreśl elementy świadczące, że to clickbait.

Przykład nr 1.

Przykład nr 2.



Twoje uwagi:

_____

_____

Moduł 2: Dezinformacja, fake newsy i zagrożenia w cyfrowej przestrzeni prywatnej

Co to jest phishing i jak go rozpoznać?

Phishing to **jedna z najczęstszych metod oszustwa w Internecie**, polegająca na **podszywaniu się pod znaną instytucję lub osobę** po to, aby wyłudzić dane, pieniądze lub dostęp do konta.
Słowo „phishing" pochodzi od angielskiego *fishing* – czyli „łowienie". Oszuści dosłownie **„łowią" ofiary**, wysyłając wiadomości, które wyglądają prawdziwie, ale są pułapką.

Najczęściej spotykane formy phishingu to:

- e-mail od rzekomego banku, który prosi o „aktualizację danych",
- SMS z informacją o „niedopłacie do przesyłki",
- wiadomość w komunikatorze od „znajomego", który prosi o pilny przelew lub kod BLIK,
- fałszywa strona logowania, która wygląda jak oryginalna, ale służy do kradzieży danych.

Najważniejsze cechy phishingu

1. **Pośpiech i presja czasu**
    - Wiadomość zawiera słowa: *natychmiast*, *pilne*, *ostatnia szansa*, *grozi utrata konta*.
    - Ma wywołać stres i skłonić do szybkiego działania.

2. **Podszywanie się pod znane instytucje**
    - Bank, urząd, firma kurierska, sklep, a nawet znajomy z Facebooka.
    - Logo i wygląd wiadomości często są identyczne jak oryginalne.
3. **Prośba o dane lub kliknięcie w link**
    - E-mail lub SMS kieruje na stronę, gdzie trzeba wpisać login, hasło, numer PESEL albo dane karty.
    - Link różni się od prawdziwego adresem, np. zamiast *bank.pl* jest *bank-secure.info*.
4. **Zbyt atrakcyjna oferta lub nagroda**
    - Informacja o wygranej, zwrocie podatku lub wyjątkowej promocji, która wymaga szybkiej reakcji.
5. **Błędy językowe i nieprofesjonalny styl**
    - Literówki, brak polskich znaków, dziwne zwroty – często wynik automatycznego tłumaczenia.

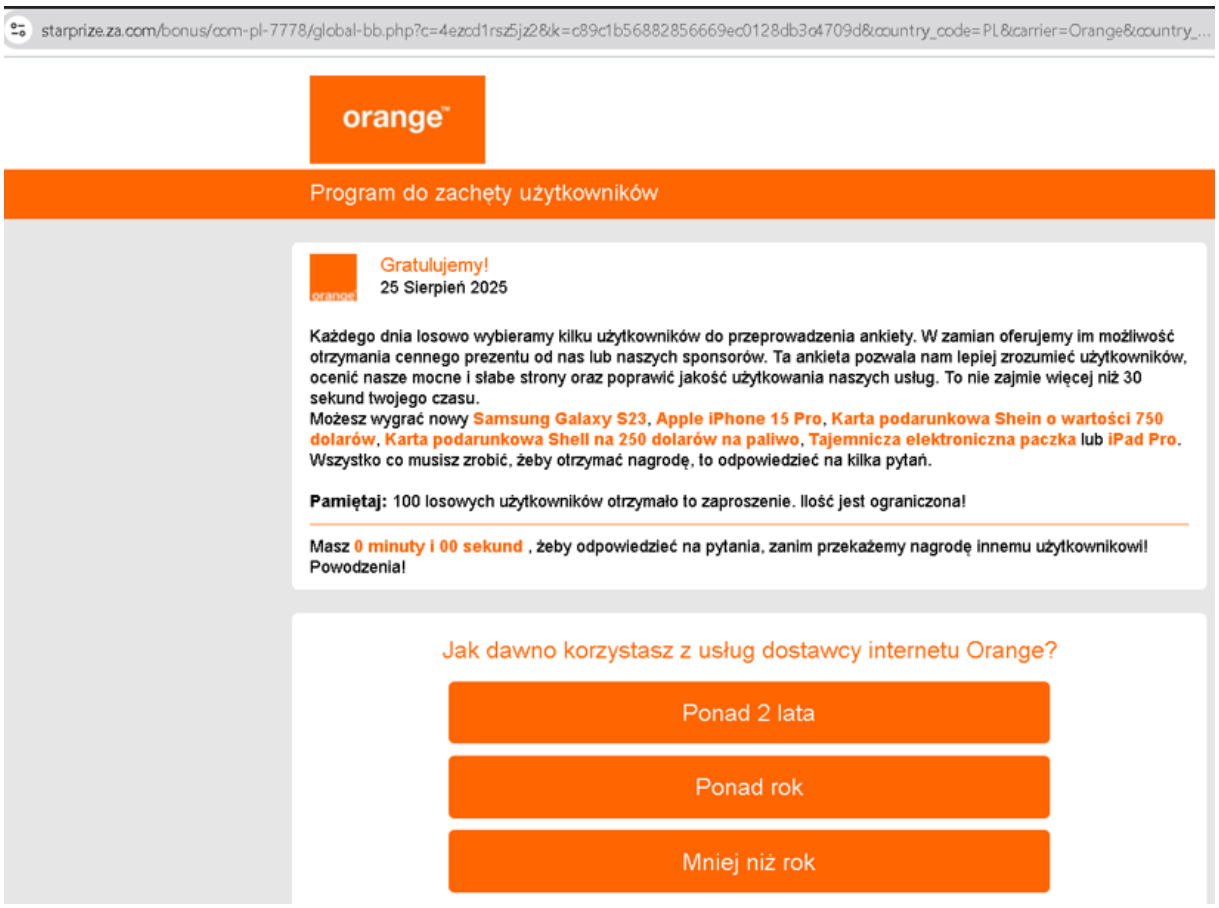
Jak się chronić przed phishingiem?

- **Nigdy nie klikaj w linki z podejrzanych wiadomości** – lepiej samodzielnie wejść na stronę banku lub firmy.
- **Nie podawaj loginów, haseł ani numerów kart** przez linki z e-maila lub SMS-a.
- **Sprawdzaj adres nadawcy** – czasem różni się tylko jednym znakiem od oryginału.
- **Zgłaszaj oszustwa** – np. na stronie https://incydent.cert.pl.

- **Zachowuj spokój** – prawdziwe instytucje nigdy nie wymagają natychmiastowego działania przez wiadomość.
-

Ćwiczenie: rozpoznawanie pishingu

Na poniższym zrzucie ekranu zaznacz elementy świadczące o tym, że jest to próba phishingu.



Moduł 3: Bezpieczeństwo cyfrowe w praktyce

Jakie dane i kiedy można udostępniać w Internecie

W Internecie zostawiamy po sobie wiele informacji, często nieświadomie. Nasze dane to nie tylko imię i nazwisko, ale także adres, numer telefonu, zdjęcia, lokalizacja, numer PESEL czy opinie, które publikujemy.
Warto pamiętać, że **każda informacja udostępniona w sieci może zostać zapisana, skopiowana i wykorzystana przez innych**, również bez naszej wiedzy.
Dlatego podstawowa zasada brzmi: **udostępniaj tylko to, co naprawdę jest potrzebne i bezpieczne.**

Dane, które można udostępniać z ostrożnością:

- **Imię i nazwisko** – gdy piszesz wiadomość lub komentarz publiczny, pamiętaj, że każdy może to zobaczyć.
- **Adres e-mail** – tylko w zaufanych miejscach, np. podczas rejestracji na znanych portalach lub w urzędach.
- **Numer telefonu** – wyłącznie wtedy, gdy jest to konieczne (np. kurier, lekarz, bank) i wiesz, kto będzie go przetwarzał.
- **Zdjęcia** – tylko takie, które nie ujawniają adresu, planu mieszkania ani wizerunku innych osób bez ich zgody.
- **Adres zamieszkania** – jedynie w prywatnych transakcjach, np. przy zakupach z dostawą, ale nigdy publicznie w komentarzach.

Dane, których nie należy udostępniać:

- **PESEL, numer dowodu osobistego, numer karty płatniczej, login i hasło** – te dane mogą posłużyć do kradzieży tożsamości lub pieniędzy.
- **Skan dokumentu tożsamości** – nie wysyłaj przez e-mail ani komunikator.

- **Dane rodzinne** – imiona dzieci, daty urodzin, miejsca pracy – to cenne informacje dla oszustów.
- **Szczegóły zdrowotne** – informacje o leczeniu, chorobach czy wynikach badań powinny pozostać prywatne.

Bezpieczeństwo sprzętu cyfrowego

Nawet najlepsze hasło i ostrożność w sieci nie wystarczą, jeśli nasz sprzęt jest źle zabezpieczony. Dlatego warto pamiętać o kilku prostych zasadach, które chronią komputer, smartfon i tablet przed wirusami, awariami i włamaniami.

Aktualizacje

Regularnie aktualizuj:

- **system** (Windows, Android, iOS),
- **przeglądarkę internetową**,
- **program antywirusowy**.

Ochrona antywirusowa i zapora

Zainstaluj **program antywirusowy** i upewnij się, że działa w tle.
Firewall (zapora sieciowa) blokuje podejrzane połączenia i chroni komputer przed włamaniem.

Porządkowanie urządzenia

Usuwaj zbędne pliki i niepotrzebne aplikacje.
W komputerze użyj „Oczyszczania dysku”, a w telefonie funkcji „Czyszczenie urządzenia”.

Zabezpieczenie dostępu

Ustaw **PIN, hasło lub wzór odblokowania**.
Nie zostawiaj urządzenia bez nadzoru i **włącz lokalizację** na wypadek kradzieży.
Przed sprzedażą telefonu **usuń wszystkie dane**.

Kopie zapasowe

Twórz **kopie zapasowe ważnych danych** w chmurze lub na pendrivie.
Zasada 3-2-1: trzy kopie, dwa nośniki, jedna poza domem.

Zasady bezpieczeństwa

- Pobieraj aplikacje tylko z oficjalnych źródeł.
- Nie klikaj w komunikaty typu „Twój komputer jest zainfekowany".

Ćwiczenie: moje zasady bezpieczeństwa

Zastanów się, jak dbasz o swoje bezpieczeństwo w Internecie i podczas korzystania z komputera lub telefonu. Zapisz **własne zasady bezpieczeństwa**, których chcesz przestrzegać.

_____

_____

_____

_____

_____

_____

_____

_____

Moduł 4: Sztuczna inteligencja – możliwości i zagrożenia w świecie informacji

Sztuczna inteligencja i jej rola w cyberbezpieczeństwie

Sztuczna inteligencja (AI) to technologia, dzięki której komputery i programy potrafią **uczyć się, rozpoznawać wzorce i podejmować decyzje podobnie jak człowiek**.
AI analizuje ogromne ilości danych, dzięki czemu może przewidywać, podpowiadać i tworzyć nowe treści – teksty, obrazy, a nawet filmy.

Pozytywna rola AI

Sztuczna inteligencja pomaga w bezpieczeństwie cyfrowym.
Dzięki niej:

- programy antywirusowe szybciej wykrywają nowe zagrożenia,
- filtry w skrzynkach e-mail rozpoznają wiadomości phishingowe,
- wyszukiwarki potrafią wykrywać fałszywe strony i ostrzegać użytkowników,
- systemy bankowe analizują transakcje i blokują podejrzane płatności.

AI może więc działać jak **cyfrowy strażnik,** który czuwa nad naszym bezpieczeństwem w sieci.

Zagrożenia związane z AI

Ta sama technologia może jednak zostać użyta w złych celach:

- do tworzenia deepfake'ów, fałszywych filmów i zdjęć wyglądających na prawdziwe,

- do generowania fake newsów i masowych komentarzy w mediach społecznościowych,
- do podszywania się pod głosy lub wizerunki prawdziwych osób.

Dlatego AI wymaga mądrego i świadomego korzystania, tak, aby służyła ludziom, a nie manipulowała nimi.

Zapamiętaj:
Sztuczna inteligencja to narzędzie – może pomagać lub szkodzić.
O tym, w jaki sposób z niej korzystamy, decyduje zawsze człowiek.

Przykłady popularnych narzędzi AI

- **ChatGPT** – pomaga pisać teksty, streszczać artykuły, tłumaczyć i odpowiadać na pytania.
- **Copilot (Microsoft)** – wspiera w pisaniu dokumentów, e-maili i prezentacji.
- **Gemini (Google)** – odpowiada na pytania, planuje, tłumaczy, pomaga w nauce.
- **Canva Magic Studio** – tworzy plakaty, grafiki i zdjęcia z wykorzystaniem AI.
- **Meta AI (Messenger, WhatsApp)** – podpowiada treści, streszcza wiadomości i pomaga w komunikacji.

Twoje notatki:

_____

_____

_____

HIGIENA CYFROWA

Korzystanie z Internetu to dziś codzienność. Czytamy wiadomości, oglądamy filmy, korzystamy z mediów społecznościowych i narzędzi sztucznej inteligencji. W tym świecie łatwo jednak natknąć się na fałszywe informacje, zmanipulowane treści czy próby oszustw. Dobra higiena cyfrowa pomaga zachować spokój, chronić siebie i innych oraz świadomie poruszać się w przestrzeni online. To zestaw prostych zasad, które chronią nasze dane, emocje i reputację.

Zasady higieny cyfrowej w sieci:

• Zanim uwierzysz w wiadomość lub film. Sprawdź źródło i autora. Fałszywe informacje często mają emocjonalne tytuły i brak wiarygodnych odnośników.

• Dbaj o prywatność, nie udostępniaj w sieci danych osobowych, numerów dokumentów, adresu zamieszkania ani informacji o swoich planach.
• Regularnie aktualizuj komputer, telefon i programy. To najlepsza ochrona przed wirusami i atakami.

• Twórz silne hasła, najlepiej zdaniowe, i nie używaj ich w kilku miejscach jednocześnie.
• Unikaj klikania w podejrzane linki, reklamy czy wiadomości o „nagrodach” i „pilnych przelewach”.

• Zachowuj dystans wobec treści generowanych przez sztuczną inteligencję. Nawet realistyczne zdjęcia i filmy mogą być fałszywe.
• Dziel się wiedzą, jeśli zauważysz oszustwo lub fake news, poinformuj bliskich, by również zachowali ostrożność.

TO UMIEM

☐ Rozpoznać fake news i wskazać elementy, które budzą wątpliwość.
☐ Odróżnić prawdziwe źródło informacji od podejrzanej strony lub autora.
☐ Rozpoznać clickbait, phishing i inne formy oszustw internetowych.
☐ Wskazać, jakie dane osobowe można udostępniać w Internecie, a jakich unikać.

☐ Zareagować właściwie na fałszywe wiadomości e-mail, SMS lub posty w mediach społecznościowych.

☐ Sprawdzić wiarygodność zdjęcia lub filmu, który może być stworzony przez sztuczną inteligencję.

☐ Korzystać bezpiecznie z narzędzi AI, nie ujawniając danych prywatnych.
☐ Tworzyć silne hasła i stosować podstawowe zasady higieny cyfrowej.
☐ Aktualizować system, program antywirusowy i przeglądarkę dla ochrony sprzętu.

☐ Dbać o bezpieczeństwo emocjonalne i informacyjne w Internecie, myśląc krytycznie zanim uwierzę lub udostępnię treść.