



# BEZPIECZNY SENIOR W CYBERŚWIECIE

Dane aktualne na dzień 29 maja 2026 r.



Ministerstwo  
Sprawiedliwości



Zadanie publiczne jest zadaniem zleconym z zakresu administracji rządowej  
i realizowane jest w oparciu o środki otrzymane z budżetu państwa

## Spis treści

|                                                               |    |
|---------------------------------------------------------------|----|
| 1.Wstęp.....                                                  | 3  |
| 2.Czym jest cyberbezpieczeństwo?.....                         | 3  |
| 3.Sztuczna inteligencja – pomoc czy zagrożenie?.....          | 4  |
| 4.Deepfake – nowe niebezpieczeństwo.....                      | 5  |
| 5.Bezpieczeństwo seniora w internecie.....                    | 6  |
| 6.Jak bezpiecznie korzystać ze sztucznej inteligencji?.....   | 7  |
| 7.AI Act – nowe prawa i ochrona użytkownika.....              | 8  |
| 8.Oszustwa internetowe najczęściej wymierzone w seniorów..... | 8  |
| 9.Jak rozpoznać próbę oszustwa?.....                          | 9  |
| 10.Prawa seniora w internecie.....                            | 9  |
| 11.Jak chronić telefon i komputer?.....                       | 10 |
| 12.Co robić w razie oszustwa?.....                            | 10 |
| 13.Najważniejsze zasady<br>bezpiecznego seniora.....          | 10 |
| Podsumowanie.....                                             | 11 |

## 1. Wstęp

---

Internet ułatwia codzienne życie:

- pozwala kontaktować się z rodziną,
- robić zakupy,
- korzystać z bankowości,
- umawiać wizyty lekarskie,
- zdobywać informacje.

Jednocześnie cyberprzestępcy coraz częściej wykorzystują nowoczesne technologie, w tym sztuczną inteligencję (AI), do oszustw i wyłudzenia danych. Dlatego każdy senior powinien znać podstawowe zasady bezpieczeństwa cyfrowego oraz wiedzieć:

- jak rozpoznawać zagrożenia,
- jak chronić swoje dane,
- jak bezpiecznie korzystać z AI,
- jakie prawa przysługują użytkownikowi internetu.

Unia Europejska wprowadza nowe przepisy dotyczące sztucznej inteligencji i bezpieczeństwa cyfrowego, w tym AI Act oraz regulacje związane z ochroną danych osobowych. Od 2025 r. obowiązuje również wymóg rozwijania kompetencji AI (AI literacy).

## 2. Czym jest cyberbezpieczeństwo?

---

Cyberbezpieczeństwo to ochrona:

- komputerów i telefonów,
- kont internetowych,
- danych osobowych,

- pieniędzy,
- prywatności.

Najczęstsze zagrożenia dla seniorów:

- oszustwa „na bank”,
- fałszywe SMS-y,
- phishing,
- wyłudzanie haseł,
- fałszywe sklepy internetowe,
- deepfake,
- podszywanie się pod rodzinę lub urzędy.

### 3. Sztuczna inteligencja – pomoc czy zagrożenie?

---

AI może pomagać seniorom:

- tłumaczyć trudne informacje,
- przypominać o lekach,
- pomagać w obsłudze urządzeń,
- wspierać kontakt z lekarzem,
- ułatwiać komunikację.

Jednak cyberprzestępcy także używają AI do:

- tworzenia fałszywych wiadomości,
- generowania realistycznych głosów,
- produkcji deepfake,
- automatycznych oszustw.

## 4. Deepfake – nowe niebezpieczeństwo

---

### Co to jest deepfake?

To wygenerowane przez AI:

- fałszywe nagrania głosu,
- filmy,
- zdjęcia,

które wyglądają jak prawdziwe.

Przestępcy mogą:

- podszyć się pod wnuczka,
- udawać pracownika banku,
- imitować głos członka rodziny.

### Zasada bezpieczeństwa

Nigdy nie podejmuj decyzji finansowych wyłącznie na podstawie:

- telefonu,
- SMS-a,
- wiadomości internetowej,
- nagrania głosowego.

Zawsze:

- oddzwoń samodzielnie,
- potwierdź informację innym kanałem,
- skonsultuj się z bliską osobą.

## 5. Bezpieczeństwo seniora w internecie

---

### 1. Nie podawaj haseł

Bank, urząd ani policja:

- nigdy nie proszą o hasło,
- nie proszą o kod BLIK,
- nie proszą o dane logowania przez telefon.

### 2. Uważaj na linki

Nie klikaj:

- podejrzanych SMS-ów,
- wiadomości o „dopłacie do paczki”,
- linków od nieznanych osób.

### 3. Chron swoje dane osobowe.

Nie publikuj publicznie:

- numeru PESEL,
- adresu,
- numeru dowodu,
- danych bankowych.

### 4. Aktualizuj urządzenia

Aktualizacje:

- poprawiają bezpieczeństwo,
- usuwają luki,
- chronią przed wirusami.

### 5. Używaj silnych haseł

Dobre hasło:

- jest długie,
- zawiera cyfry i znaki,
- nie zawiera daty urodzenia.

Najlepiej używać różnych haseł do różnych kont.

## 6. Jak bezpiecznie korzystać ze sztucznej inteligencji?

---

### 1. AI nie zawsze mówi prawdę.

Chatbot może:

- pomylić fakty,
- podać nieaktualne informacje,
- stworzyć błędną odpowiedź.

Dlatego:

- sprawdzaj informacje,
- korzystaj z wiarygodnych źródeł,
- nie ufaj ślepo AI.

### 2. Nie wpisuj poufnych danych.

Do publicznych narzędzi AI nie należy wpisywać:

- danych medycznych,
- numerów kont,
- danych logowania,
- dokumentów prywatnych.

### 3. Uważaj na fałszywe aplikacje AI.

Cyberprzestępcy tworzą:

- fałszywe chatboty,

- niebezpieczne aplikacje,
- strony podszywające się pod znane firmy.

#### **4. Pobieraj aplikacje wyłącznie z oficjalnych sklepów.**

- Google Play,
- Apple App Store.

## **7. AI Act – nowe prawa i ochrona użytkownika**

Unia Europejska stworzyła AI Act – pierwsze kompleksowe przepisy dotyczące sztucznej inteligencji. Regulacje weszły w życie etapami od 2024 i 2025 roku. Co oznacza to dla seniora?

Nowe przepisy mają:

- zwiększyć bezpieczeństwo użytkowników,
- ograniczyć niebezpieczne systemy AI,
- wymagać większej przejrzystości,
- chronić obywateli przed manipulacją.

## **8. Oszustwa internetowe najczęściej wymierzone w seniorów**

### **„Na wnuczka”**

Przestępca:

- podszywa się pod rodzinę,
- prosi o pilny przelew,
- wywołuje emocje i presję czasu.

### **„Na bank”**

Fałszywy konsultant:

- informuje o „ataku na konto”,

- prosi o dane logowania,
- nakłania do instalacji programu.

## 9. Jak rozpoznać próbę oszustwa?

---

### Sygnaly ostrzegawcze:

- presja czasu,
- prośba o tajemnicę,
- żądanie pieniędzy,
- błędy językowe,
- dziwny adres strony,
- podejrzanе wiadomości,
- nietypowy telefon od „banku”.

**Najważniejsza zasada:** Nie działaj pod wpływem emocji.

## 10. Prawa seniora w internecie

---

Każdy użytkownik ma prawo do:

- ochrony danych osobowych,
- prywatności,
- informacji o wykorzystaniu AI,
- bezpieczeństwa cyfrowego,
- zgłaszania naruszeń.

W wielu przypadkach użytkownik powinien wiedzieć, że:

- rozmawia z AI,
- treść została wygenerowana automatycznie,
- obraz lub głos są sztucznie wygenerowane.

## 11. Jak chronić telefon i komputer?

---

### Podstawowe zasady:

- używaj programu antywirusowego,
- ustaw blokadę ekranu,
- nie instaluj nieznanych aplikacji,
- rób kopie zapasowe danych,
- korzystaj z bezpiecznego Wi-Fi.

## 12. Co robić w razie oszustwa?

---

### Jeśli podano dane lub wykonano przelew:

- Skontaktuj się z bankiem.
- Zmień hasła.
- Zgłoś sprawę na policję.
- Poinformuj rodzinę.
- Zabezpiecz wiadomości i dokumenty.

Im szybsza reakcja, tym większa szansa na ograniczenie strat.

## 13. Najważniejsze zasady bezpiecznego seniora

---

### Zawsze:

- ✓ sprawdzaj informacje,
- ✓ pytaj bliskich o pomoc,
- ✓ aktualizuj urządzenia,
- ✓ zachowuj ostrożność,

- ✓ korzystaj z oficjalnych stron i aplikacji,
- ✓ chroń dane osobowe.

### **Nigdy:**

- ✗ nie podawaj haseł,
- ✗ nie wysyłaj kodów BLIK obcym,
- ✗ nie klikaj podejrzanych linków,
- ✗ nie ufaj nieznanym rozmówcom,
- ✗ nie działaj pod presją czasu.

## **Podsumowanie**

---

Cyberświat daje seniorom ogromne możliwości:

- kontakt z rodziną i dostęp do usług,
- edukację,
- wygodę codziennego życia.

Jednocześnie rozwój sztucznej inteligencji powoduje nowe zagrożenia:

- deepfake,
- oszustwa internetowe,
- manipulację i wyludzanie danych.

Dlatego najważniejszą ochroną stają się:

- wiedza i kompetencje cyfrowe,
- ostrożność,
- umiejętność rozpoznawania zagrożeń.

Bezpieczny senior w cyberświecie to nie osoba, która zna się na technologii perfekcyjnie, lecz taka, która potrafi korzystać z niej świadomie i odpowiedzialnie.

## **PUNKT NIEODPŁATNEGO PORADNICTWA W JAWORZNIE PROWADZONY PRZEZ STOWARZYSZENIE “DOGMA”**

### **Punkt Nieodpłatnego Poradnictwa Obywatelskiego i Mediacji**

Zespół Szkół Ponadpodstawowych nr 4

ul. Armii Krajowej 5 (Osiedle Stałe)

Poniedziałek - piątek 15.00-19.00

*Wtorek, czwartek i piątek - mediacja*

## **INNE PUNKTY PORADNICZE W JAWORZNIE**

### **Punkt Nieodpłatnego Poradnictwa Obywatelskiego i Mediacji**

Szkoła Podstawowa nr 13 w Jaworznie

ul. Urzędnicza 11 (Śródmieście)

Poniedziałek - piątek 15.30-19.30

*Czwartek i piątek - mediacja*

### **Punkt Nieodpłatnego Poradnictwa Obywatelskiego i Mediacji**

Szkoła Podstawowa nr 7 w Jaworznie

ul. Ławczana 12 (Podłęże)

Poniedziałek - piątek 15.30-19.30

*Środa i czwartek - mediacja*

---

## **ZAPISY NA PORADY**

- telefonicznie pod nr tel. 510-970-680 w godzinach pracy urzędu
- elektronicznie poprzez stronę <https://zapisy-np.ms.gov.pl/>
- osobiście – w urzędzie



Ministerstwo  
Sprawiedliwości



Zadanie publiczne jest zadaniem zleconym z zakresu administracji rządowej  
i realizowane jest w oparciu o środki otrzymane z budżetu państwa