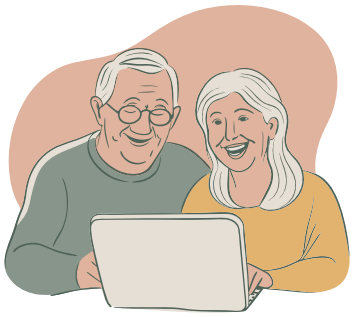


Sztuczna inteligencja dla każdego

Przewodnik bezpiecznego korzystania z AI dla seniorów

Kompleksowy przewodnik dla seniorów: Ochrona danych osobowych podczas korzystania z technologii AI

Ten przewodnik zawiera podstawowe informacje, które pomogą seniorom zrozumieć, jakich danych osobowych nigdy nie należy udostępniać systemom sztucznej inteligencji (AI). Choć AI oferuje wiele korzyści, ochrona prywatności i danych osobowych pozostaje najważniejsza, zwłaszcza w dzisiejszym cyfrowym świecie, w którym AI jest coraz częściej integrowana z codziennymi technologiami.

Zrozumienie AI i ryzyk dla prywatności

Czym jest AI i jak wykorzystuje Twoje dane?

Sztuczna inteligencja odnosi się do systemów komputerowych zaprojektowanych do wykonywania zadań, które zwykle wymagają ludzkiej inteligencji. Obejmuje to asystentów głosowych, chatboty, zautomatyzowane systemy obsługi klienta i bardziej zaawansowane aplikacje. Większość systemów AI opiera się w dużej mierze na danych, aby funkcjonować i się uczyć, co rodzi istotne kwestie dotyczące prywatności użytkowników, zwłaszcza seniorów.

Dofinansowane przez Unię Europejską

Crea360

ENABLER

Kiedy wchodzisz w interakcję z AI, często udostępniasz informacje, które te systemy zbierają, przechowują i potencjalnie wykorzystują w przyszłości. Modele AI działające w chmurze, takie jak popularne chatboty, mogą przechowywać dostarczone informacje bezterminowo, a te dane mogą potencjalnie zostać użyte do trenowania innych modeli AI. Przechowywanie danych osobowych tworzy różnorodne ryzyka związane z prywatnością i bezpieczeństwem, o których seniorzy powinni wiedzieć.

Dlaczego seniorzy muszą być szczególnie ostrożni

Seniorzy są często celem oszustów, a wraz z rozwojem technologii, AI uczyniła te oszustwa bardziej wyrafinowanymi i przekonującymi. Przestępcy mogą teraz używać AI do tworzenia bardzo realistycznych klonów głosów, deepfake'ów wideo oraz przekonujących fałszywych stron internetowych, które wyglądają na legalne. Te technologiczne postępy sprawiają, że coraz trudniej jest odróżnić prawdziwą komunikację od oszukańczej, co zwiększa ryzyko wykorzystania seniorów.

Dane osobowe, których nigdy nie należy udostępniać AI

Informacje finansowe

Nigdy nie udostępniaj danych finansowych systemom AI, chyba że korzystasz z bezpiecznej, zweryfikowanej aplikacji bankowej. Obejmuje to:

- Numery kart kredytowych, daty ważności i kody bezpieczeństwa (CVV)
- Numery kont bankowych i informacje o przelewach
- Dane logowania do bankowości internetowej i hasła
- Informacje o kontach inwestycyjnych
- Numery identyfikacji podatkowej lub zeznania podatkowe

Udostępnienie danych finansowych niezaufanym systemom AI może prowadzić do kradzieży tożsamości, nieautoryzowanych transakcji i poważnych strat finansowych. Nawet legalne systemy AI mogą przechowywać te dane w sposób, który może zostać naruszony.

Dofinansowane przez Unię Europejską

Crea360 ENABLER

Informacje medyczne i zdrowotne

Twoje informacje zdrowotne są wyjątkowo wrażliwe i należy je chronić. Unikaj udostępniania:

- Diagnoz medycznych i historii leczenia
- Informacji o przepisywanych lekach
- Danych o ubezpieczeniu zdrowotnym i numerach polis
- Wyników badań medycznych
- Informacji dotyczących zdrowia psychicznego

Dokumentacja medyczna zawiera bardzo osobiste informacje o stanie zdrowia i leczeniu. Jeśli trafią one w niepowołane ręce, mogą zostać niewłaściwie wykorzystane, np. wpływać na ubezpieczenie lub prowadzić do dyskryminacji.

Dokumenty tożsamości i numery identyfikacyjne

Chroń te kluczowe identyfikatory przed systemami AI:

- Numery identyfikacyjne (PESEL w Polsce, DNI w Hiszpanii)
- Numery ubezpieczenia społecznego
- Dane z paszportów lub dowodów osobistych
- Informacje z prawa jazdy
- Akty urodzenia lub dokładne daty urodzenia w połączeniu z innymi danymi osobowymi

Dokumenty i numery są głównym celem złodziei tożsamości i powinny być udostępniane wyłącznie oficjalnym instytucjom lub zweryfikowanym dostawcom usług, gdy jest to absolutnie konieczne.

Dokumenty prawne i informacje

Dokumenty prawne często zawierają wrażliwe dane osobowe, które należy chronić:

- Testamenty i dokumenty dotyczące planowania spadkowego
- Pełnomocnictwa
- Akty własności i tytuły nieruchomości
- Umowy i kontrakty prawne
- Dokumenty sądowe lub ugody

Dofinansowane przez Unię Europejską

Crea360 ENABLER

Dokumenty te często zawierają kombinacje danych osobowych, które mogą zostać wykorzystane. Ponadto mogą obejmować kwestie prywatne, które powinny pozostać poufne.

Informacje o zabezpieczeniach domowych

Twoje bezpieczeństwo fizyczne może być zagrożone przez udostępnienie:

- Szczegółów dotyczących systemu zabezpieczeń domu
- Adresu domowego połączonego z informacją, kiedy nie ma Cię w domu
- Informacji o cennych przedmiotach i miejscu ich przechowywania
- Kluczy lub kodów dostępu do mieszkania

Ujawnienie tych informacji może narazić Cię na kradzież lub włamanie, szczególnie jeśli przestępcy ustalą, że nie ma Cię w domu.

Specyficzne zagrożenia prywatności związane z AI dla seniorów

Urządzenia z asystentem głosowym i dane głosowe

Urządzenia z asystentem głosowym zyskały popularność wśród seniorów ze względu na wygodę i dostępność. Jednak te urządzenia nagrywają i przetwarzają dane głosowe, co rodzi kilka obaw dotyczących prywatności:

- Twój głos może zostać sklonowany już na podstawie krótkiej próbki dźwięku
- Nagrania głosu mogą zawierać rozmowy w tle lub wrażliwe informacje
- Systemy AI mogą przechowywać dane głosowe bezterminowo, jeśli nie zmienisz ustawień prywatności

Aby bezpiecznie korzystać z tych urządzeń, zapoznaj się z ustawieniami prywatności i rozważ wyłączenie funkcji nagrywania głosu, gdy nie są potrzebne. Bądź szczególnie czujny wobec nieautoryzowanych połączeń z prośbą o wypowiedzenie się lub potwierdzenie głosu – mogą to być próby uzyskania próbki do klonowania głosu.

Dofinansowane przez Unię Europejską

Crea360 ENABLER

Oszustwa AI wymierzone w seniorów

Sztuczna inteligencja stworzyła nowe możliwości dla oszustów, by atakować seniorów poprzez:

Oszustwa z klonowaniem głosu

Oszuści mogą teraz odtworzyć czyjś głos na podstawie krótkiej próbki, co sprawia, że rozmowa wydaje się pochodzić od bliskiej osoby. Technologia ta jest tak zaawansowana, że fałszywy głos może być niemal nie do odróżnienia od prawdziwego.

Na przykład, 82-letni mężczyzna odebrał telefon od rzekomego zięcia. Dzwoniący, używając klonowanego głosu stworzonego przez AI, twierdził, że ma problemy z prawem i potrzebuje 17 000 złotych na kaucję. Mężczyzna wypłacił pieniądze, zanim odkrył, że to oszustwo.

Deepfake'i

AI może generować realistyczne filmy i obrazy, które sprawiają wrażenie, że zaufana osoba popiera oszukańczą inwestycję lub wysyła pilną prośbę. Są one szczególnie przekonujące, gdy wydają się pochodzić od członków rodziny lub autorytetów.

Fałszywe strony internetowe i phishing

Przestępcy tworzą niemal identyczne kopie legalnych stron internetowych, oszukując użytkowników, by wprowadzili wrażliwe informacje. AI sprawia, że te fałszywe strony są coraz bardziej zaawansowane i trudniejsze do rozpoznania.

Jak się chronić podczas korzystania z AI

Weryfikuj zanim zareagujesz

Jeśli otrzymasz telefon lub wiadomość od osoby podającej się za członka rodziny lub urzędnika z prośbą o pieniądze lub dane osobowe – rozłącz się i oddzwoń na znany numer. Ten prosty krok może zapobiec wielu oszustwom.

Ustal rodzinne hasło bezpieczeństwa

Ustal hasło, którego członkowie rodziny mogą używać, by potwierdzić tożsamość w rozmowach telefonicznych lub wiadomościach. Dodaje to dodatkową warstwę weryfikacji, której oszust nie zna.

Dofinansowane przez Unię Europejską

Crea360

ENABLER

Podchodź sceptycznie do pilnych próśb

Oszuści często wywołują poczucie pilności, by uniemożliwić racjonalne myślenie. Daj sobie czas na zweryfikowanie każdej pilnej prośby, zwłaszcza dotyczącej pieniędzy lub danych osobowych.

Dostosuj ustawienia prywatności urządzeń AI

Wiele urządzeń AI ma konfigurowalne ustawienia prywatności, które pozwalają kontrolować, jakie dane są zbierane i jak są używane. Warto poświęcić czas na ich poznanie i odpowiednią konfigurację.

Zrozumienie ochrony danych osobowych w UE w kontekście AI

Unia Europejska wprowadziła kompleksowe przepisy chroniące prywatność danych osobowych, które dotyczą także systemów AI:

Ochrona wynikająca z RODO i Aktu o AI

O gólne rozporządzenie o ochronie danych (RODO) i Akt o AI współdziałają w ochronie danych osobowych. Zgodnie z tymi regulacjami:

- Masz prawo wiedzieć, jak Twoje dane osobowe są przetwarzane
- Organizacje muszą uzyskać odpowiednią zgodę przed zebraniem i wykorzystaniem danych
- Masz prawo do dostępu do swoich danych i żądania ich usunięcia
- Obowiązują szczególne zakazy nadużywania AI w sposób szkodliwy dla jednostki

Inicjatywy krajowe

Hiszpania niedawno wdrożyła rozwiązania chroniące prywatność w technologiach cyfrowych, w tym aplikację umożliwiającą weryfikację wieku bez udostępniania nadmiarowych danych. Polski urząd ochrony danych osobowych (UODO) pracuje nad zapewnieniem zgodności przepisów AI z prawem o ochronie danych osobowych.

Europejska Rada Ochrony Danych (EDPB) powołała również grupę roboczą ds. egzekwowania przepisów dotyczących AI, aby rozwiązywać problemy związane z prywatnością w całej UE, co pokazuje zaangażowanie UE w ochronę danych obywateli w erze AI.

Dofinansowane przez Unię Europejską

Crea360 ENABLER

Podsumowanie: Równowaga między korzyściami a ryzykiem

Sztuczna inteligencja oferuje wiele korzyści dla seniorów, w tym monitorowanie zdrowia, pomoc w codziennych zadaniach i kontakt społeczny. Jednak te korzyści muszą być zrównoważone ryzykiem dla prywatności poprzez świadome i ostrożne korzystanie z AI.

Zrozumienie, jak chronić dane osobowe, rozpoznawanie potencjalnych oszustw oraz wdrożenie praktycznych środków bezpieczeństwa pozwoli seniorom czerpać korzyści z AI, minimalizując ryzyka prywatności i bezpieczeństwa.

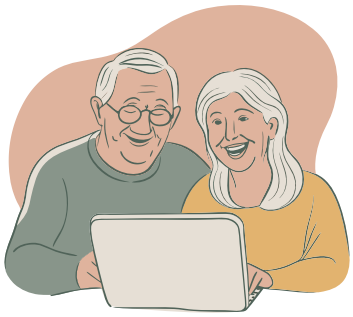
Pamiętaj, że choć technologia rozwija się szybko, podstawowe zasady ochrony danych osobowych pozostają niezmienne: bądź czujny, weryfikuj przed udostępnieniem, a w razie wątpliwości – skonsultuj się z zaufaną osobą lub oficjalnym źródłem.

Kluczem do bezpiecznego poruszania się po świecie AI nie jest unikanie technologii, lecz korzystanie z niej świadomie i z odpowiednimi zabezpieczeniami prywatności. Dzięki odpowiedniej wiedzy i ostrożności seniorzy mogą z ufnością korzystać z zalet AI, chroniąc jednocześnie swoje dane osobowe.

***

Dofinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Fundacja Rozwoju Systemu Edukacji. Unia Europejska ani Fundacja Rozwoju Systemu Edukacji nie ponoszą za nie odpowiedzialności.

Materiały zostały opracowane w ramach projektu „Sztuczna inteligencja dla każdego" – zastosowania AI w codzienności Seniora. dofinansowanego ze środków Unii Europejskiej w programie Erasmus+, typ akcji: AKCJA 2 Partnerstwa na rzecz współpracy, Partnerstwa na małą skalę (KA210-ADU) w sektorze Edukacja Dorosłych, numer wniosku: 2024-2-PL01-KA210-ADU-000287353.



Artificial Intelligence for everyone

A guide to the safe use of AI for seniors

A comprehensive guide for seniors: Protecting your personal information when using AI technologies

This guide provides essential information to help seniors understand what personal information should never be shared with artificial intelligence (AI) systems. While AI offers many benefits, protecting your privacy and personal data remains paramount, especially in today's digital world where AI is increasingly integrated into everyday technologies.

Understanding AI and privacy risks

What is AI and how does it use your data?

Artificial intelligence refers to computer systems designed to perform tasks that typically require human intelligence. This includes voice assistants, chatbots, automated customer service systems, and more sophisticated applications. Most AI systems rely heavily on data to function and learn, which raises important privacy considerations for users, especially seniors.

When you interact with AI, you're often sharing information that these systems collect, store, and potentially use for future operations. Cloud-hosted AI models, like popular chatbots, may retain the information you provide indefinitely, and this data could potentially be used to train other AI models. This retention of personal information creates various privacy and security risks that seniors should be aware of.

Co-funded by the European Union

Crea360

ENABLER

Why seniors need to be particularly careful

Seniors are frequently targeted by scammers, and with advances in technology, AI has made these scams more sophisticated and convincing. Criminals can now use AI to create highly realistic voice clones, deepfake videos, and convincing fake websites that appear legitimate. These technological advancements make it increasingly difficult to distinguish genuine communications from fraudulent ones, placing seniors at heightened risk of exploitation.

Personal information you should never share with AI

Financial information

Never share your financial details with AI systems unless you're using a secure, verified banking application. This includes:

- Credit card numbers, expiration dates, and security codes (CVV)
- Banking account numbers and routing information
- Online banking credentials and passwords
- Investment account information
- Tax identification numbers or tax returns

Sharing financial information with unverified AI systems could lead to identity theft, unauthorised transactions, and significant financial loss. Even legitimate AI systems may store this data in ways that could be compromised.

Medical and health information

Your health information is highly sensitive and should be protected. Avoid sharing:

- Medical diagnoses and treatment histories
- Prescription medication information
- Health insurance details and policy numbers
- Medical test results
- Mental health information

Medical records contain deeply personal information about your health conditions and treatments. This information could be misused if it falls into the wrong hands, potentially affecting your insurance coverage or leading to discrimination.

Co-funded by the European Union

Crea360

ENABLER

Personal identification documents and numbers

Protect these critical identity markers from AI systems:

- National identification numbers (PESEL in Poland, DNI in Spain)
- Social Security numbers
- Passport or identity card details
- Driver's license information
- Birth certificates or exact birth dates combined with other personally identifiable information

These documents and numbers are prime targets for identity thieves and should only be shared with official government agencies or verified service providers when absolutely necessary.

Legal documents and information

Legal documents often contain sensitive personal information that should be safeguarded:

- Wills and estate planning documents
- Power of attorney forms
- Property deeds and titles
- Contracts and legal agreements
- Court documents or settlement agreements

These documents frequently contain combinations of personal information that could be exploited. Additionally, they may include private matters that should remain confidential.

Home security information

Your physical safety could be compromised by sharing:

- Home security system details
- Home address combined with when you're away from home
- Information about valuable possessions and where they're kept
- Keys or access codes to your residence

Revealing this information could make you vulnerable to physical theft or home invasions, particularly if criminals can determine when you're not at home.

Co-funded by the European Union

Crea360

ENABLER

AI-Specific privacy concerns for seniors

Voice-Assisted devices and voice data

Voice-assisted devices have become popular among seniors for their convenience and accessibility. However, these devices record and process voice data, raising several privacy concerns:

Your voice can be cloned with as little as a short audio sample

Voice recordings may contain background conversations or sensitive information

AI systems may store voice data indefinitely unless privacy settings are adjusted

To use these devices safely, familiarise yourself with privacy controls and consider turning off voice recording features when not needed. Be especially vigilant about unauthorised calls requesting you to speak or confirm your voice, as these could be attempts to gather audio for voice cloning.

AI-Generated scams targeting seniors

Artificial intelligence has created new avenues for scammers to target seniors through:

Voice cloning scams

Scammers can now replicate a person's voice using just a short audio clip, making it seem as though a loved one is calling for help or in trouble. This technology is so advanced that the fake voice can be nearly indistinguishable from the real person.

For example, an 82-year-old man was recently targeted with a phone call that appeared to be from his son-in-law. The caller, using AI-generated voice cloning, claimed to be in legal trouble and needed $17,000 for bail. The man withdrew the money before discovering it was a scam.

Deepfake scams

AI can generate realistic videos and images that make it appear that a trusted figure is endorsing a fraudulent investment or sending an urgent request. These can be particularly convincing when they appear to come from family members or authority figures.

Fake websites and phishing

Co-funded by the European Union

Crea360

ENABLER

Criminals create nearly identical copies of legitimate websites, tricking users into entering sensitive information. AI makes these fake sites increasingly sophisticated and harder to identify.

Protecting yourself when using AI technologies

Verify before taking action

If you receive a call or message from someone claiming to be a family member or official requesting money or personal information, hang up and call them back directly using a known phone number. This simple step can prevent many scams.

Establish a family code word

Have a safe word that family members can use to confirm their identity during calls or messages. This adds an additional layer of verification that AI scammers would not know.

Be skeptical of urgent requests

Scammers often create a false sense of urgency to prevent you from thinking critically. Take time to verify any urgent requests, especially those involving money transfers or personal information.

Adjust privacy settings on AI devices

Many AI devices come with customisable privacy settings that allow you to control what data is collected and how it is used. Take time to understand and configure these settings to protect your information.

Understanding EU Data Protection for AI

The European Union has established comprehensive regulations to protect individuals data privacy, which apply to AI systems:

GDPR and AI Act Protections

The General Data Protection Regulation (GDPR) and the AI Act work together to protect your personal data. Under these regulations:

- You have the right to know how your personal data is being processed
- Organisations must obtain proper consent before collecting and

using your data

- You have the right to access your data and request its deletion
- There are specific prohibitions against misusing AI in ways that could harm individuals

Country-specific initiatives

Spain has recently implemented privacy-preserving solutions for digital technologies, including an app that allows users to verify their age without sharing excessive personal information. Poland's data protection authority (UODO) is working to ensure compatibility between AI regulations and personal data protection laws.

The European Data Protection Board (EDPB) has also created a task force on AI enforcement to address privacy concerns across the EU, demonstrating the EU's commitment to protecting citizens data in the age of AI.

Conclusion: Balancing Benefits and Risks

Artificial intelligence offers many benefits for seniors, including health monitoring, assistance with daily tasks, and social connection. However, these benefits must be balanced against privacy risks through informed and cautious use.

By understanding what personal information to protect, recognising potential scams, and implementing practical safety measures, seniors can enjoy the advantages of AI while minimising privacy and security risks. Remember that while technology advances rapidly, the fundamental principles of protecting your personal information remain constant: be vigilant, verify before sharing, and when in doubt, seek help from trusted family members or official sources.

The key to safely navigating the AI landscape is not avoiding technology altogether, but rather using it mindfully and with appropriate privacy protections in place. With the right knowledge and precautions, seniors can confidently embrace the benefits of AI while keeping their personal information secure.

Co-funded by the European Union

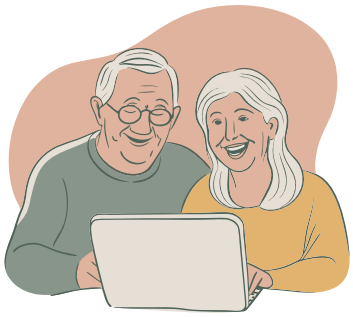
Crea360

ENABLER

⁂

Co-financed by the EU. The views and opinions expressed are those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System can be held responsible for them.

The materials were developed as part of the project 'Artificial Intelligence for Everyone' - AI applications in seniors' daily life, co-financed by the European Union under the Erasmus+ program, Action Type: ACTION 2 Partnerships for Cooperation, Small-scale Partnerships (KA210-ADU) in the Adult Education sector, application number: 2024-2-PL01-KA210-ADU-000287353.



Inteligencia Artificial para todos

Una guía para el uso seguro de la de la IA para personas mayores

Guía integral para personas mayores: Proteger su información personal al utilizar tecnologías de inteligencia artificial

Esta guía proporciona información esencial para ayudar a las personas mayores a comprender qué información personal nunca debe compartirse con los sistemas de inteligencia artificial (IA). Si bien la IA ofrece muchos beneficios, proteger su privacidad y sus datos personales sigue siendo primordial, especialmente en el mundo digital actual donde la IA se integra cada vez más en las tecnologías cotidianas.

Comprender la IA y los riesgos para la privacidad

¿Qué es la IA y cómo utiliza sus datos?

La inteligencia artificial se refiere a sistemas informáticos diseñados para realizar tareas que normalmente requieren inteligencia humana. Esto incluye asistentes de voz, chatbots, sistemas automatizados de atención al cliente y aplicaciones más sofisticadas. La mayoría de los sistemas de IA dependen en gran medida de los datos para funcionar y aprender, lo que plantea importantes consideraciones sobre la privacidad para los usuarios, especialmente las personas mayores.

Cuando interactúa con la IA, a menudo está compartiendo información que estos sistemas recopilan, almacenan y posiblemente utilizan para operaciones futuras. Los modelos de IA alojados en la nube, como los chatbots populares, pueden conservar la información que usted proporciona de manera inde-

Cofinanciado por la Unión Europea

Crea360 ENABLER

finida, y estos datos podrían utilizarse para entrenar otros modelos de IA. Esta retención de información personal crea diversos riesgos para la privacidad y la seguridad que las personas mayores deben tener en cuenta.

Por qué las personas mayores deben tener especial cuidado

Las personas mayores son frecuentemente blanco de estafadores, y con los avances en tecnología, la IA ha hecho que estas estafas sean más sofisticadas y convincentes. Los delincuentes pueden ahora utilizar IA para crear clones de voz altamente realistas, videos deepfake y sitios web falsos que parecen legítimos. Estos avances tecnológicos hacen que sea cada vez más difícil distinguir las comunicaciones genuinas de las fraudulentas, lo que pone a las personas mayores en mayor riesgo de ser explotadas.

Información personal que nunca debe compartir con la IA

Información financiera

Nunca comparta sus datos financieros con sistemas de IA a menos que esté utilizando una aplicación bancaria segura y verificada. Esto incluye:

- Números de tarjetas de crédito, fechas de vencimiento y códigos de seguridad (CVV)
- Números de cuentas bancarias e información de ruta
- Credenciales y contraseñas de banca en línea
- Información sobre cuentas de inversión
- Números de identificación fiscal o declaraciones de impuestos

Compartir información financiera con sistemas de IA no verificados podría conducir al robo de identidad, transacciones no autorizadas y pérdidas económicas significativas. Incluso los sistemas de IA legítimos pueden almacenar estos datos de forma que puedan ser vulnerados.

Información médica y de salud

Su información de salud es altamente sensible y debe protegerse. Evite compartir:

- Diagnósticos médicos e historiales de tratamiento
- Información sobre medicamentos recetados
- Detalles y números de pólizas de seguros de salud

Cofinanciado por la Unión Europea

Crea360 ENABLER

- Resultados de pruebas médicas
- Información sobre salud mental

Los registros médicos contienen información profundamente personal sobre sus condiciones de salud y tratamientos. Esta información podría ser mal utilizada si cae en manos equivocadas, afectando potencialmente su cobertura de seguro o dando lugar a discriminación.

Documentos de identificación personal y números

Proteja estos marcadores críticos de identidad frente a los sistemas de IA:

- Números de identificación nacional (PESEL en Polonia, DNI en España)
- Números de seguridad social
- Detalles de pasaportes o carnés de identidad
- Información de licencias de conducir
- Actas de nacimiento o fechas exactas de nacimiento combinadas con otra información personal identificable

Estos documentos y números son objetivos principales para los ladrones de identidad y solo deben compartirse con agencias gubernamentales oficiales o proveedores de servicios verificados cuando sea absolutamente necesario.

Documentos e información legal

Los documentos legales a menudo contienen información personal sensible que debe protegerse:

- Testamentos y documentos de planificación patrimonial
- Formularios de poderes notariales
- Escrituras y títulos de propiedad
- Contratos y acuerdos legales
- Documentos judiciales o acuerdos de conciliación

Estos documentos frecuentemente contienen combinaciones de información personal que podrían ser explotadas. Además, pueden incluir asuntos privados que deben permanecer confidenciales.

Cofinanciado por la Unión Europea

Crea360 ENABLER

Información sobre seguridad en el hogar

Su seguridad física podría verse comprometida al compartir:

- Detalles del sistema de seguridad del hogar
- Dirección del domicilio combinada con información sobre cuándo no está en casa
- Información sobre objetos valiosos y dónde se guardan
- Llaves o códigos de acceso a su residencia

Revelar esta información podría hacerle vulnerable a robos o allanamientos, especialmente si los delincuentes logran determinar cuándo no se encuentra en casa.

Preocupaciones específicas sobre la privacidad relacionadas con la IA para personas mayores

Dispositivos con asistencia por voz y datos de voz

Los dispositivos con asistencia por voz se han vuelto populares entre las personas mayores por su conveniencia y accesibilidad. Sin embargo, estos dispositivos graban y procesan datos de voz, lo que plantea varias preocupaciones sobre la privacidad:

- Su voz puede ser clonada con tan solo una muestra corta de audio
- Las grabaciones pueden contener conversaciones de fondo o información sensible
- Los sistemas de IA pueden almacenar datos de voz indefinidamente, a menos que se ajusten las configuraciones de privacidad

Para usar estos dispositivos de forma segura, familiarícese con los controles de privacidad y considere desactivar las funciones de grabación de voz cuando no sean necesarias. Sea especialmente cuidadoso con llamadas no autorizadas que le pidan hablar o confirmar su voz, ya que podrían ser intentos de recopilar audio para clonación de voz.

Estafas generadas por IA dirigidas a personas mayores

La inteligencia artificial ha creado nuevas vías para que los estafadores se dirijan a las personas mayores mediante:

Estafas con clonación de voz

Los estafadores ahora pueden replicar la voz de una persona usando solo un clip de audio corto, haciendo que parezca que un ser querido llama pidiendo ayuda o está en problemas. Esta

tecnología es tan avanzada que la voz falsa puede ser casi indistinguible de la persona real.

Por ejemplo, un hombre de 82 años fue recientemente víctima de una llamada que parecía ser de su yerno. El interlocutor, utilizando una clonación de voz generada por IA, afirmó tener problemas legales y necesitar 17.000 dólares para la fianza. El hombre retiró el dinero antes de descubrir que se trataba de una estafa.

Estafas con deepfakes

La IA puede generar videos e imágenes realistas que hacen parecer que una figura de confianza está respaldando una inversión fraudulenta o enviando una solicitud urgente. Estas pueden ser particularmente convincentes cuando parecen provenir de familiares o figuras de autoridad.

Sitios web falsos y phishing

Los delincuentes crean copias casi idénticas de sitios web legítimos, engañando a los usuarios para que ingresen información sensible. La IA hace que estos sitios falsos sean cada vez más sofisticados y difíciles de identificar.

Protegerse al utilizar tecnologías de IA

Verifique antes de actuar

Si recibe una llamada o mensaje de alguien que dice ser un familiar o funcionario solicitando dinero o información personal, cuelgue y devuélvale la llamada directamente utilizando un número conocido. Este paso simple puede evitar muchas estafas.

Establezca una palabra clave familiar

Tenga una palabra de seguridad que los miembros de la familia puedan usar para confirmar su identidad durante llamadas o mensajes. Esto añade una capa adicional de verificación que los estafadores con IA no conocerían.

Desconfíe de las solicitudes urgentes

Los estafadores suelen crear una falsa sensación de urgencia para evitar que piense con claridad. Tómese el tiempo para verificar cualquier solicitud urgente, especialmente las que impliquen transferencias de dinero o información personal.

Cofinanciado por la Unión Europea

Crea360 ENABLER

Ajuste la configuración de privacidad en dispositivos con IA

Muchos dispositivos de IA tienen configuraciones de privacidad personalizables que le permiten controlar qué datos se recopilan y cómo se utilizan. Tómese el tiempo para entender y configurar estas opciones para proteger su información.

Comprender la protección de datos en la UE en relación con la IA

La Unión Europea ha establecido regulaciones integrales para proteger la privacidad de los datos personales, que se aplican a los sistemas de IA:

Protecciones del RGPD y la Ley de IA

El Reglamento General de Protección de Datos (RGPD) y la Ley de Inteligencia Artificial trabajan conjuntamente para proteger sus datos personales. Según estas regulaciones:

- Tiene derecho a saber cómo se están procesando sus datos personales
- Las organizaciones deben obtener su consentimiento adecuado antes de recopilar y utilizar sus datos
- Tiene derecho a acceder a sus datos y solicitar su eliminación
- Hay prohibiciones específicas contra el uso indebido de la IA de formas que puedan dañar a las personas

Iniciativas específicas por país

España ha implementado recientemente soluciones que preservan la privacidad en tecnologías digitales, incluida una aplicación que permite a los usuarios verificar su edad sin compartir información personal excesiva. La autoridad de protección de datos de Polonia (UODO) está trabajando para garantizar la compatibilidad entre las regulaciones sobre IA y las leyes de protección de datos personales.

La Junta Europea de Protección de Datos (EDPB) también ha creado un grupo de trabajo sobre la aplicación de la IA para abordar preocupaciones sobre privacidad en toda la UE, lo que demuestra el compromiso de la UE con la protección de los datos de los ciudadanos en la era de la IA.

Cofinanciado por la Unión Europea

Crea360 ENABLER

Conclusión: Equilibrar beneficios y riesgos

La inteligencia artificial ofrece muchos beneficios para las personas mayores, incluidos el monitoreo de la salud, la asistencia en las tareas diarias y la conexión social. Sin embargo, estos beneficios deben equilibrarse con los riesgos para la privacidad mediante el uso informado y cauteloso.

Al comprender qué información personal debe protegerse, reconocer posibles estafas e implementar medidas prácticas de seguridad, las personas mayores pueden disfrutar de las ventajas de la IA mientras minimizan los riesgos para su privacidad y seguridad.

Recuerde que aunque la tecnología avanza rápidamente, los principios fundamentales de protección de su información personal permanecen constantes: esté alerta, verifique antes de compartir y, en caso de duda, busque ayuda de familiares de confianza o fuentes oficiales.

La clave para navegar con seguridad el mundo de la IA no es evitar la tecnología por completo, sino usarla conscientemente y con las protecciones de privacidad adecuadas. Con el conocimiento y las precauciones correctas, las personas mayores pueden adoptar con confianza los beneficios de la IA mientras mantienen segura su información personal.

*
**

Cofinanciado por la UE. Los puntos de vista y opiniones expresados son los del autor o autores y no reflejan necesariamente los puntos de vista y opiniones de la Unión Europea o la Fundación para el Desarrollo del Sistema Educativo. Ni la Unión Europea ni la Fundación para el Desarrollo del Sistema Educativo son responsables de ellos.

Los materiales fueron desarrollados como parte del proyecto 'Inteligencia Artificial para Todos' - aplicaciones de IA en la vida diaria de las personas mayores, cofinanciado por la Unión Europea en el marco del programa Erasmus+, Tipo de Acción: ACCIÓN 2 Asociaciones para la Cooperación, Asociaciones a pequeña escala (KA210-ADU) en el sector de la Educación de Adultos, número de solicitud: 2024-2-PL01-KA210-ADU-000287353.