Organization for Security and Co-operation in Europe
Mission to Bosnia and Herzegovina

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

SAFE USE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS

A SHORT GUIDE FOR CITIZENS



Disclaimer

The preparation of this document was supported by the OSCE Mission to BiH. Any point of view, statement or opinion expressed in this document, if not explicitly indicated as coming from the OSCE Mission to BiH, does not necessarily reflect the official policy of the OSCE Mission to BiH.

What is Artificial Intelligence?

Artificial intelligence, or AI, is a term used to describe technologies and systems that demonstrate intelligent behaviour by analysing available data and taking certain actions with a certain degree of autonomy. AI systems can also generate content and perform tasks that once required human work and intelligence, such as creating text, recognising speech, summarising information, translating, or developing various plans and projects.

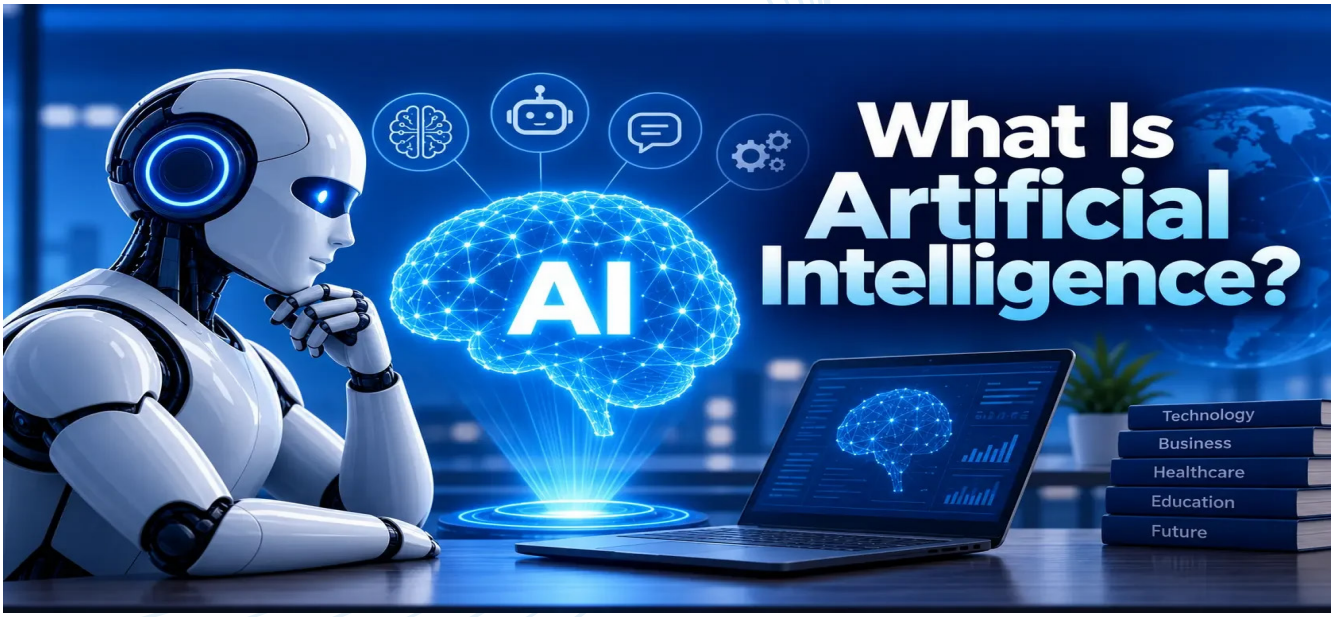
Artificial intelligence is a major achievement of the rapid technological development and an effective tool available to people in today's world.

In everyday life, AI can be useful for drafting various texts, processing topics, explaining concepts in almost any field, comparing products, translating, and generating ideas for planning travel, home improvements, business activities, and processes in many areas of life and work.

How to Use AI Smartly and Safely

AI can help us analyse information, generate ideas and support decision-making, while continuously using learning methods to achieve optimal results. However, AI does not understand situations in the same way humans do and does not possess ethical judgement or responsibility. It therefore cannot replace logical thinking, human judgement, experience or decision-making.

Since AI does not perceive information in the same way humans do, it can produce inaccurate, incomplete or misleading results. AI-generated answers should therefore always be critically assessed and verified, particularly when dealing with sensitive topics such as **health, finances, employment, legal matters, security, human rights, or family and children.**



Main Risks

In general, various assessments and analyses of the use of AI tools identify several recurring risks:

- AI can generate inaccurate information and present it as fact, It can reproduce or intensify bias;
- It can be misused to create convincing scams, false content and manipulative messages;
- Risks also arise when users enter personal, sensitive or confidential information into AI tools, as such information may be stored or processed in ways the user does not expect.

In addition, on social media and other online platforms, the problem is not only that content can be easily produced, but also that algorithms often favour content that attracts and holds attention and engagement. Such content is not necessarily the most accurate, useful or reliable.

In BiH linguistic and social context, additional caution is needed: AI may misunderstand **language nuances, humour, irony, hate speech or historical context. This means that something that AI identifies as "neutral", "normal" or "safe", may in reality be inaccurate, harmful, discriminatory or manipulative.**

Practical Tips for Safer Use

When using AI, ask yourself three (3) questions:

Does AI provide the source of the information?

Is the information still accurate and up to date?

How can I verify its accuracy and reliability?

This is particularly important when there is a possibility that information might affect your health, finances, privacy, reputation or security. A professionally written message should never discourage you from checking the content and its context.

RECOMMENDED	WHAT NOT TO DO
Use AI for ideas, drafts, explanations and summarising information.	Do not leave the final decision on an important matter to AI.
Ask for the source and date of the answer.	Do not trust the first answer simply because it sounds convincing or professional.
Use general and anonymous examples when asking AI questions.	Do not enter personal, health, financial or other confidential information.
If AI recommends a website or link, check the domain, sender and context.	Do not immediately open links contained in urgent or unexpected messages.
Download applications and files only from official and trusted sources.	Do not install an application or add-on simply because AI recommended it.
Be transparent if AI helped you write or process content.	Do not present AI-assisted content as entirely your own work.
Warn others if you notice a new type of scam or deception.	Do not keep information to yourself if sharing it could help others recognise or avoid a scam.

Privacy and Personal Data

The most important rule is: **Do not enter into public AI tools anything that you would not make public or share with a stranger.**

This includes your full name, address, telephone number, email address, national identification number or other identification number, banking details, health information, information about children, as well as other people's personal information.

It is equally important to protect business information. Internal documents, meeting minutes, emails, contracts, legal information, source code, business strategies, tables containing customer, employee or partner data, as well as documents that could reveal the identity of a person or organisation “through context”, should not be entered into publicly available AI tools. Even when you remove a person's name, they may still be identifiable through the date, location, description of an event or a combination of details.

If you really need to describe a real-life case to an AI tool, use **general and non-identifiable descriptions.** Instead of real names and details, use terms such as **“Person A”, “a colleague”, “an employee” or “a user”,** and remove all unnecessary identifiers.

Before using an AI tool, check its privacy settings, chat history and whether there is an option in the settings to prevent your data from being used to improve the model.

It is Important to Recognise AI Scams and Deepfake Content

Generative AI has made it easier for scammers to create messages, photographs, voice recordings and videos that appear convincing. Today, it is relatively easy to create AI-generated content that looks or sounds as though it comes from someone you trust.

Be particularly cautious if you receive a call or voice message in which someone sounds like a family member, friend or supervisor and urgently asks you to make a payment, provide information or take some other unusual action.

The main warning signs remain the same: the message is **unexpected,** demands an **immediate response,** attempts to create **fear, sympathy or panic,** asks for **money, a password, account access or documents,** and wants you to act **immediately without verification.**

Today, better grammar, more professional design or a convincing voice do not automatically make a message safe - ask yourself whether the message makes sense, whether you were expecting it, and whether it is trying to influence your decision.

If you receive a voice message or an unexpected call, **do not call back using the number or link provided in the message** and do not act immediately. Call the person or institution using a number you already know, or contact them through a separate communication channel. If a video, photograph or audio recording seems “convincing”, this is a reason for additional verification, not for a faster response.

At work, follow internal rules and do not transfer business data to publicly available services without authorisation and assessment. Use only approved AI tools and accounts.

If AI suggests that you download an application, game, add-on, book or file, first check whether it actually exists and download it only from an official app store or a verified provider. Do not install anything “blindly” simply because AI recommended it.

Children and AI

Children are increasingly using AI for school, information searches and entertainment, so it is important that the rules are simple and clear. UNICEF recommends that parents and caregivers **explore AI together with children,** discuss the answers provided by AI tools, explain what AI can and cannot do, protect children's privacy, and develop critical thinking by checking answers and sources.

Children should understand that AI can support learning, but it should not become a shortcut that replaces thinking. UNICEF explicitly advises using AI as a useful tool rather than as a substitute for one's own thinking, and recommends that parents review with their children what the tool collects and shares.

For children and young people, an additional rule applies: AI does not replace friends, parents, teachers or professional support.

Parents - please do not automatically ban children from using AI. Instead, learn together and set clear boundaries.

What to Do If You Have Been a Victim

If you suspect that you have fallen victim to an AI-assisted scam or have entered your information on a fake website, **first stop all communication.** Then **change your passwords,** especially for accounts connected to e-mail, banking or social media. For banking details, **contact your bank immediately.**

Save the evidence, including screenshots, messages, the number from which the call originated, links and the time of the incident. If you believe that a criminal offence or other unlawful activity has occurred, **report the case** to the police or the relevant authority. Finally, **warn others.** Information about scams should be shared with family, colleagues and friends, because the same scam campaign is usually sent to a large number of people.

Quick Self-Check

Before I Enter Something into AI

- ☐ I know which AI tool I am using and what I am using it for.
- ☐ I have checked the privacy settings and chat history.
- ☐ I am not entering personal, health, financial or confidential business information
- ☐ If I am describing a real-life case, I have anonymised it.

Before I trust an Answer

- ☐ I have checked the date and source.
- ☐ I have compared the answer with at least one other reliable source.
- ☐ I have asked myself: does this make sense in the real-world context?
- ☐ I know that a professional tone does not mean that the answer is accurate.

Before I Click, Download or Send

- ☐ I have checked the domain and sender.
- ☐ I do not click on urgent or unexpected messages without verification.
- ☐ If AI recommends a tool or application, I first check the official source.
- ☐ My devices and applications are up to date.

If a Message Asks for Money, a Password or Documents

- ☐ I stop and do not react immediately.
- ☐ I verify the request through another communication channel.
- ☐ I do not rely solely on a video, voice message or photograph.
- ☐ If I suspect a scam, I stop communicating.

If I think I Have Been a Victim

- ☐ I change my passwords.
- ☐ If my banking information has been compromised, I contact my bank.
- ☐ I save the evidence.
- ☐ I report the incident to the police and relevant authorities.
- ☐ I warn people around me.

Short FAQ

Can I trust an AI answer if it sounds confident and professional?

Do not trust it completely or automatically. AI can provide a convincing but inaccurate answer, so always check the source, date and context.

Can I copy a contract, official e-mail or data table into AI?

Not into a public AI tool, unless this has been explicitly authorised, assessed and appropriately protected. This is particularly important for personal data and confidential information.

How can I recognise an AI-assisted scam?

Look for signs of urgency, pressure, requests for money or passwords, unexpected contact, and messages that try to prevent you from verifying information through another channel.

Can children use AI on their own?

Children can use AI with clear rules, discussion and age-appropriate supervision. The most important aspects are privacy, checking answers and understanding that AI is not a substitute for their own thinking.

Should I say that I used AI to prepare projects?

Yes, particularly at school, at work, in public communications, presentations, translations and research. Transparency builds trust.

