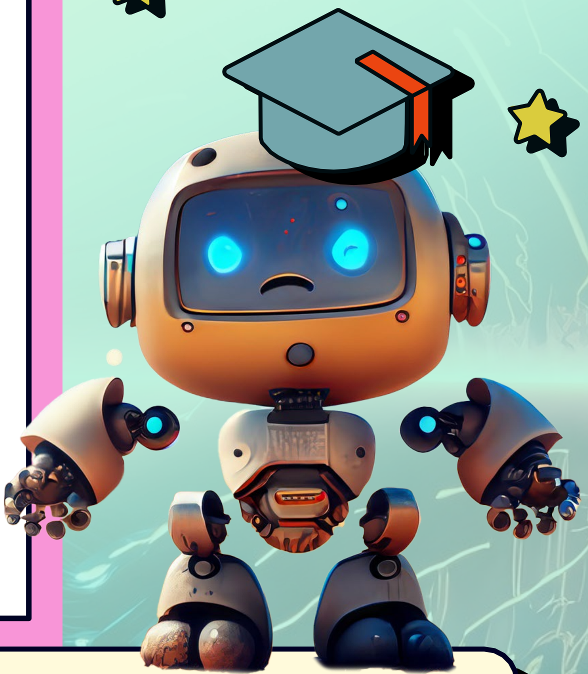
Using Artificial Intelligence Safely and Securely

Artificial intelligence (AI) is taking over the working world and is gradually becoming an everyday tool for more and more employees — be it for creating documents, images, or code. However, if used carelessly, AI can also pose risks, for example, with regard to data protection, copyright issues, or liability for possible damage. Additionally, cybercriminals also use AI to generate malicious code, forge images, videos or voices, and to generate and spread false news. In this document, you will learn some key tips to use AI safely and protect yourself against new threats from cybercriminals.

Generative AI

When people talk about a revolution in artificial intelligence, they are usually referring to technologies based on generative artificial intelligence. What does that mean? Generative AI essentially consists of two components: a large volume of training data and a neural network. This is an algorithm that can independently learn from the training data and generate new content from it. Well-known examples of generative AI tools include ChatGPT and Bard for texts and code or Midjourney, DALL-E, and Synthesia for artificially generated images and videos.



AI, the Latest Weapon for Cybercriminals

Cybercriminals are already using generative AI to create deceptively realistic phishing emails that trick users into careless, dangerous actions, such as clicking on a link or inputting confidential data or passwords. Another danger is malicious code created by AI, which is often no longer recognized by conventional diagnostic programs. Finally, generative AI is also used to create and spread false news containing fake photos and videos (deepfakes). Here’s what to keep in mind:

- Continue to follow your usual behavior: Never carelessly click on links in suspicious emails and never reveal your passwords.
- Always keep your work computer, personal computer, smartphone, tablet, and other devices up to date and install security updates promptly.
- Always check the source of news stories, especially on social media.
- Learn how to recognize fake images and videos by paying attention to any abnormalities or deviations in the hands, teeth, or facial expressions of the people depicted.
- Learn more and stay updated with the latest insights by taking security awareness training.

AI At Work: Data Protection, Copyright, Liability

When used correctly, generative AI can increase efficiency and simplify planning and work for employees in almost all areas of an organization. However, clear rules should be defined and followed prior to use. In particular, this impacts data protection, copyright, and the question of liability. Here’s what you should remember:

✓ **Data protection:** Exercise caution when entering data into an AI system. In case of doubt, assume that all information might be visible to the providers of these applications or to other users. Consequently, never enter any personal data relating to employees, applicants, or customers, such as addresses, names, or dates of birth. This also applies to confidential data about your organization’s products, technologies, and innovations.

✓ **Copyright:** You cannot claim copyright for text and images that you have created entirely using AI. Only products created by humans may be protected by copyright. Important: Always be transparent with customers and your organization as to whether something was generated using AI.

✓ **Liability:** In the event of an accident or damage as a result of a product that was created using AI, such as software code, you are personally liable, and not the manufacturer of the AI system. It is therefore important that you check the results thoroughly, especially in the case of critical applications or products.