

JOINT ADVISORY BY THE CYBER SECURITY AGENCY OF SINGAPORE AND INFOCOMM MEDIA DEVELOPMENT AUTHORITY

SAFE & SECURE USE OF GENERATIVE AI FOR INDIVIDUALS

Background

1. Generative Artificial Intelligence (Gen AI) tools — such as chatbots, image generators, and virtual assistants — are becoming a part of our everyday life. These tools can boost productivity, spark creativity, help with learning, and simplify complex tasks. However, they also introduce new risks to personal privacy, information accuracy, and digital well-being.
2. This advisory highlights three best practices for individuals to use Gen AI tools safely and securely. First, to safeguard your information when using Gen AI. Second, to verify the content received from Gen AI before using or sharing further. Third, to maintain healthy boundaries when engaging with AI. As new tools and platforms emerge, users should stay informed about the risks and capabilities of these new technologies, to inform how they can continue to use them safely and securely.

#1 Safeguard Your Information when Using Gen AI

3. Users might be inclined to provide more information to Gen AI tools to make them more useful and personalised, for example asking for travel recommendations for your particular age group and interests. Over time, even casual conversations with Gen AI tools can reveal a lot about you. If the tools are compromised, such information could fall in the wrong hands and used for malicious purposes like fraud or scams.
 - a. **Control what you share.** Once you share information with Gen AI tools, you lose control over how it is stored, processed, or accessed. Avoid disclosing personal details that you would ordinarily keep private. This includes your full name, address, and NRIC number, as well as sensitive information such as financial or medical records. Workplace information and confidential or sensitive business data should also never be provided to Gen AI tools without proper authorisation.
 - b. **Choose your Gen AI tools carefully.** Use reputable tools with clear privacy policies and terms of service (ToS). Review the ToS carefully to understand how your data is managed and what permissions you are granting. Otherwise, assume all information shared with a Gen AI tool can be accessed by the platform provider and that your conversations may be used to train AI models. **This includes Gen AI accessed through third-party apps**, such as unofficial mobile apps or browser extensions, which may also collect and use your data. When using these apps, watch for red flags such as excessive permission requests that do not match the app's intended function (e.g., requesting camera access or location data) or apps from unknown developers. These could indicate potentially harmful applications designed to collect your personal information.

#2 Verify Content from Gen AI Tools before Using or Sharing

4. Legitimate Gen AI tools are designed with safety mechanisms ('guardrails') that aim to minimise or prevent harmful content, potential biases, and provide appropriate disclaimers for sensitive topics like medical or legal advice. However, guardrails are not foolproof, and Gen AI tools can still produce unsafe or inappropriate content. Gen AI tools are also known to generate false content known as confabulations or 'hallucinations'. These are fictional or partially correct information presented to users in a convincing and authoritative manner, which can come in the form of fabricated references, quotes, or statistics that appear credible.

- a. **Cross-check content with official and trusted sources.** Approach AI-generated content with a critical mindset. Verify the generated content, just as you would with any other source, with legitimate sources such as government websites. For high-impact issues like health and legal advice, consult with professionals. Treat AI-generated content as a starting point, not the final word.
- b. **Pause before using or sharing.** Ask yourself whether the information makes sense and can be confirmed before making a decision. If you encounter content that seems harmful, misleading, or manipulative, report it to the respective authority. Providing this information to the platform provider can also help them to improve their Gen AI tools and protect other users.

#3 Maintain Healthy Boundaries when Engaging with AI

5. Constant engagement with Gen AI to conduct research or make recommendations can help to build familiarity and confidence in using such tools. Because such engagements take place through conversations with Gen AI, it may start to appear as a convenient friend that understands or empathises with you, but such interactions are simply a product of pattern recognition in the AI model.

- a. **Use AI as a tool, not to replace real-world relationships.** For some user groups, such as younger users, it can be more difficult to tell the difference between genuine emotional connections with real people and responses that are generated by AI. Over time, this can create emotional dependency, and in turn reduce the time and effort they invest in building and maintaining real-world relationships. Parents and caregivers should help children understand that **while Gen AI tools are fun and helpful, AI is a tool for support or learning rather than as a replacement for genuine human connection.**

For further guidance on AI companions and their impact, refer to the comprehensive Digital for Life advisory here: <https://www.digitalforlife.gov.sg/learn/resources/all-resources/ai-companions-ai-chatbot-risks>

- b. **Use AI to augment, not replace your thinking.** AI can help you to explore ideas or gain new perspectives, but it cannot replace your critical thinking and decision-making. Be discerning about tasks that can be delegated to AI (e.g., making trip itineraries) and those that should remain under your control (e.g., making important life decisions). Over-relying on Gen AI tools may also pose a risk to personal skill development, particularly in education, where students may miss out on honing creativity, critical thinking, and reasoning abilities.

Looking Ahead

6. Gen AI tools will increasingly be integrated in our lives in various ways, from research and analysis to simplifying tasks. However, using such tools safely and securely requires informed and mindful use, to protect against potential downsides such as loss of sensitive information, or exposure to incorrect or harmful content.

7. **Safeguard your information when using Gen AI tools, verify Gen AI content before using and sharing further, and maintain healthy boundaries when engaging with AI.** As AI continues to evolve, stay informed and adaptable in your approach when interacting with AI.

Further Reading

- <https://www.digitalforlife.gov.sg/learn/resources/all-resources/ai-companions-ai-chatbot-risks>
- <https://www.digitalforlife.gov.sg/learn/resources/all-resources/understand-risks-associated-with-gen-ai>
- <https://www.tech.gov.sg/technews/generative-ai-where-can-it-go-wrong>
- <https://isomer-user-content.by.gov.sg/61/908918b6-a9f5-4494-a980-6f93ec6b3f13/ai-infographic-v2-how-does-singapore-law-treat-ai-generated-content-that-may-infringe-copyright.pdf>
- <https://www.adalovelaceinstitute.org/blog/ai-companions/>
- <https://time.com/7346052/problem-ai-flattering-us/>