Using AI safely and responsibly

GET SAFE ONLINE .org

www.getsafeonline.org

The hidden dangers of AI in the online world

Whether we like it or not, AI (Artificial Intelligence) has become part of daily life for most internet users.

When we shop, share, watch, listen, date or the many other things we do online, chances are that AI is working in the background to both enhance your experience and influence your choices.

And, of course, many of us use publicly available AI tools routinely to write, design, research and compare.

One thing's for sure: AI is here to stay. But are you confident that you and your family are using it safely and responsibly? Here are some of the issues facing internet users all the time:

- Being deceived by an AI-generated or modified image or video of a person or event, or a fraudulent advertisement for a product or service that doesn't actually exist
- Placing excessive trust in AI-generated information without verifying it from other sources, including news and political influencing
- Having difficulty differentiating between reality and false or inaccurate information, again without verifying

- Sharing too much personal or confidential information when using AI platforms
- Acting too readily on AI-driven buying recommendations and product reviews
- Overreliance on AI at the expense of thinking through a solution (and therefore using one's own brainpower)
- At work, relying on AI to do the job instead using one's expertise, experience and initiative
- In education, relying on AI to produce assignments and other coursework. This can undermine personal growth, lead to potential disciplinary actions and erode trust. Educators and recruiters are increasingly adopting AI detection software, increasing the risk of being caught out.

Cybercrime and AI

Scammers regularly use AI to create highly convincing emails, texts, voice messages and deepfake videos that mimic official communications from banks, government departments, trusted business or political leaders or people you meet when online dating. This includes automating and personalising phishing attempts, pulling data from social media and public records to create messages that appear to be targeted and genuine. These messages also generally don't contain the spelling and grammatical mistakes that were typical of previous types of scams.

Your top three CHECKS to spot AI-assisted scams

- **CHECK the context:** Be suspicious of unsolicited emails, messages or phone calls – even if they seem authentic. They could be fraudulent.
- **CHECK the details:** The spelling and grammar in AI-generated content may be perfect, but it sometimes includes inconsistencies, such as slightly odd email addresses, incorrect logos or unusual phrasing. In images and videos, check for signs of things not being quite as they should.
- **CHECK identity independently:** Don't rely on just a message. Call or message the person or company using contact details you know to be correct, to check if the sender is genuine.

Top tips to use AI safely and responsibly

Don't over-rely on AI:
Let it help brainstorm or summarise, but always review and refine the content yourself to maintain authenticity and integrity. Be sure to validate information by checking other, trusted sources.

Look after your personal information:
Avoid inputting sensitive personal or financial information into AI tools. Your details could be revealed to other people using generative AI or search tools.

Stay informed:
Keep abreast of advances in AI, including the latest tactics used by scammers and malicious influencers. Your awareness is a powerful defence.

AI is a powerful tool, but you need to stay alert and use it responsibly so that you can enjoy its benefits while minimising the risks.

#UsingAISafely

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to **Report Fraud** at **www.reportfraud.police.uk** or by calling **0300 123 2040**. If you are in Scotland, contact **Police Scotland** on **101**.

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

airbnb · BARCLAYS · barclaycard · UK International Development (Partnership | Progress | Prosperity) · ARMY BE THE BEST · LLOYDS · HALIFAX · BANK OF SCOTLAND · viagogo · Llywodraeth Cymru Welsh Government · Report Fraud · NPCC National Police Chiefs' Council · NATIONAL TRADING STANDARDS Protecting Consumers Safeguarding Businesses · Renfrewshire Council · cifas · neighbourhood ALERT · METROPOLITAN POLICE · HEDDLU GOGLEDD CYMRU NORTH WALES POLICE · Ofcom · VS VICTIM SUPPORT · TO STOP FRAUD · NEIGHBOURHOOD WATCH