



AI April Fools



Scammers use AI to fake, steal, fool, and scam

As artificial intelligence becomes ever more powerful, scammers use it to craft convincing deepfakes, impersonate trusted contacts, and trick people into sharing sensitive information. Meanwhile, millions of people are feeding AI tools sensitive personal or work-related data without understanding where it goes.

To bring awareness to this growing concern, the [National Cybersecurity Alliance](#) is using the month of April to focus on combatting AI-powered scams.

Why AI Fools matters

AI is already here, bringing innovation...but also risks:

- **AI-powered scams are harder to spot:** Deepfakes and AI-generated phishing emails look more real than ever.
- **People are oversharing with AI tools:** The National Cybersecurity Alliance's 2025 [Oh Behave survey](#) finds that 43% of users have shared sensitive work information with AI without their employer's knowledge!
- **Misinformation factories:** AI can generate realistic but completely false text, image, and video content, making it harder to tell fact from fiction.
- **Easier for scammers:** Scammers only need 15 seconds, sometime less, of audio/video to create fakes.

Oh Behave!

The National Cybersecurity Alliance's 2025 [2025 Oh Behave survey](#) found that:

- **58%** of users report receiving **no training on security or privacy risks** associated with these technologies.
- **43%** of users have **shared sensitive work information** with AI without their employer's knowledge.

Can you Outsmart the AI Scammers?

To help build awareness with this growing concern, the National Cybersecurity Alliance has stood up "[Outsmart the AI Scammers](#)". This site hosts a few tests to see how well you can identify Human vs AI. It also provides links to resources covering:

- How AI Scams Work
- How to Set Up a Safe Word
- Extra Verification Steps

Additional Resources

- [Does AI Take Your Data? AI and Data Privacy](#)
- [AI and the Future of Phishing: Interactive Tool](#)
- [Why Your Family and Coworkers Need a Safe Word in the Age of AI](#)
- [How to Protect Yourself Against Deepfakes](#)



The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.