

## AI-Powered Scams: Don't Be the Next Victim

Cybersecurity Awareness Month serves as a reminder that safeguarding our data is more crucial than ever. This year, we highlight a new threat: AI-driven scams. These scams utilize artificial intelligence to deceive, impersonate, and defraud people more quickly and convincingly than ever before.

AI-driven scams employ tools like chatbots, deepfakes, and language models (such as ChatGPT) to automate and customize fraud. These scams:

- Mimic human writing to craft fake emails.
- Use deepfake audio to impersonate leaders.
- Automate phishing to amplify attack volume.
- Send AI-generated phishing emails that sound legitimate, even without spelling errors or grammatical mistakes.

Why are these scams more effective?

- Messages are customized for individuals using collected data.
- Victims feel they are speaking with someone they trust.
- AI mimics tone, style, and urgency.
- Phishing emails have shifted from sloppy, error-filled spam to highly realistic messages powered by AI text generators.

How can you protect yourself and your DCH?

- Pause before responding to emails or messages requesting urgent actions.
- Verify voices and videos through a second channel.
- Call the person directly and look for tone or behavior that feels unusual compared to past interactions.
- Never click on unknown links, even if they appear legitimate.
- Always use Multi-Factor Authentication (MFA).
- Report suspicious activity to IT or security.

AI-powered scams are evolving rapidly. But so can our awareness. During this Cybersecurity Awareness Month, take a few moments to question what you see, hear, and read because, in the age of AI, your best defense is a skeptical mind.