Article: AI-powered scams and what you can do about them

KEY POINTS:

- Various AI-driven scams are becoming increasingly sophisticated, including:
  - *Deepfake Audio and Video*: Scammers use AI to create realistic but fake audio and video clips that can mislead victims into believing they are genuine.
    - It's is only in the last year or two that advances in the tech have allowed a new voice to be generated from as little as a few seconds of audio.
    - This type of scam has already been done using President Biden's voice. They caught the culprits behind that, but future scammers will be more careful.
  - *Phishing Attacks*: AI-generated text makes phishing emails and messages more convincing and harder to detect.
  - *Fake News Propagation*: AI helps create and spread false information rapidly, making it challenging to discern truth from fiction.

- Prevention Measures: To safeguard against these scams, the article suggests:
  - Cybersecurity 101 is your best bet to make sure that your accounts are adequately protected against the most obvious attacks.
  - *Be Skeptical of Unsolicited Communications*: Treat unexpected messages with caution, especially those that urge immediate action.
  - *Use Multi-factor authentication (MFA)*: Adding an extra verification step can protect your accounts from unauthorized access.
  - *Keep Software Updated*: Regularly updating your software can defend against known security flaws.
  - *Educate Yourself and Others*: Being aware of common scam tactics can help you recognize and avoid them.