PROTECT YOURSELF AGAINST A.I. SCAMS

CRIME PREVENTION: MEDINA POLICE DEPARTMENT

AI is becoming increasingly sophisticated, and scammers are using it to their advantage. Here are a few ways that AI is being used to scam people:

- Voice cloning scams: Scammers are using AI to clone the voices of real people, such as your friends or family members. This makes it much more believable when they call you and ask for money or personal information.
- Fake news scams: AI can be used to create fake news articles that look like they're from legitimate sources. This can be used to spread misinformation and scare people into acting, such as clicking on a link or giving up their personal information.
- Phishing scams: AI can be used to create phishing emails that look like they're from legitimate companies. These emails often contain links that, when clicked, will take you to a fake website that looks like the real thing. Once you enter your personal information on the fake website, the scammer can steal it.
- Deepfake scams: AI can be used to create deepfakes, which are videos or images that have been manipulated to make it look like someone is saying or doing something they never said or did. These deepfakes can be used to damage someone's reputation or to scam people out of money.

Here are some tips to help you protect yourself from AI-based scams:

- Be suspicious of any unsolicited calls or emails. If you don't know who the caller or sender is, don't answer the call or open the email.
- Use a strong password and change it regularly. You should also use a different password for each website or online service you use.
- Be aware of the latest scams. You can find information about the latest scams on the websites of the Federal Trade Commission (FTC) and the Cybersecurity and Infrastructure Security Agency (CISA).
- If you receive a call from someone claiming to be from a government agency or a legitimate company, ask them to provide their name, title, and department. You can then verify their identity by calling the company or agency directly.
- If you receive an email from someone claiming to be from a government agency or a legitimate company, don't click on any links in the email. Instead, go to the company's website directly and log in to your account.

If you think you've been scammed, report it to the Federal Trade Commission (FTC).
You can do this online at ftc.gov/complaint or by calling 1-877-FTC-HELP.

Medina Police Department: For emergencies, call 911 – Office (425) 233-6420