June 2025 Cyber Security Tip: Artificial Intelligence - Social Engineering Attacks

As artificial intelligence (AI) evolves, malicious actors are leveraging these new capabilities, such as the elimination of misspelling and grammar errors, to craft realistic phishing emails, text messages, and scams.

Malicious actors can now purchase Malware as a Service (MaaS) to help them gather socially engineered content from social media sites to make realistic emails or texts that contain malicious intent.

Key takeaway: AI has significantly transformed the landscape of phishing attacks by making them more sophisticated, personal, and harder to detect. Be diligent in reviewing the content and intention of each message to ensure you do not fall victim to a malicious actor.

OFFICE OF
CYBER SECURITY
MISSOURI OFFICE *of* ADMINISTRATION

Watch for the following signs of malicious intent when receiving content:

- Be cautious of emails that convey a sense of urgency or that could include consequences.
- Review any links that look suspicious or contain misspellings. Be especially suspicious of links that ask you to provide credentials.
- Be wary of requests to provide sensitive information such as your personally identifiable information, or data that would not normally be publicly provided.
- Carefully analyze requests that ask you to make a purchase. Be particularly suspicious if asked to purchase a gift card or to alter payment account information.

Additional security tips:

- Do not trust voices or videos sent in emails or text messages.
- Always verify through a trusted source if you receive anything questionable. If you receive an email that sounds out of character for a trusted source, follow up with them. Do not use contact information contained in the original email.
- Use the report phishing button if you receive anything suspicious.