September 2025 Cyber Security Tip: Image Security

Images uploaded to online resources are being used by malicious actors leveraging artificial intelligence (AI) to fool individuals or help them identify weaknesses to exploit people and systems. Understanding the risks when posting pictures online will help protect you from becoming a victim.

Digital images contain metadata—date, time, and location—that can be exploited. For example, posting a vacation photo online reveals your location and when you were there, which can be used to execute advanced social engineering attacks. It is recommended to remove or disable the creation of metadata before sharing pictures online.

AI can analyze images to detect physical security issues in a home like the presence of security cameras, the quality of lighting, or other physical security weaknesses. Do not post pictures of your building's technology or infrastructure online.

When uploading photos to "free" apps or services, the terms of service that you agree to often grant the company the right to use your images for training their AI models. Data, such as the backgrounds of your photos, can be used for highly specific and invasive ad targeting.

OFFICE OF CYBER SECURITY
MISSOURI OFFICE of ADMINISTRATION

Key takeaway: Be aware of the sensitivity of data being captured in photos before you post them online and ensure that they do not contain sensitive information.