

Hook, line and stinker

Travel photos now reveal a mine of personal information to scammers courtesy AI.

Mathures Paul reports

After returning from Lisbon, Portugal, you post a few personal photographs on social media. There is no mention of the city in the location tag. There is nothing out of the ordinary to give away the place where the photos were clicked.

Soon, you get a message, perhaps referencing your bank, mentioning that suspicious activity was detected "while travelling internationally". You have always been careful about keeping personal details very private. You do what any sensible person would do — click on the link to confirm that your card wasn't compromised.

Welcome to the world of personalised scam messages. That stash of holiday pictures has helped scammers, who are using artificial intelligence to analyse images to find the minutest of details, like a signpost that's almost invisible or a part of an address on shop signage.

McAfee Labs, the threat research and intelligence division of the cybersecurity

identify the location. People need to think beyond metadata and consider what the photo itself may be revealing," says Grobman.

To find out what's at play, McAfee built an automated testing pipeline and ran it against a dataset of 21,236 travel images in the public domain. The company also conducted a separate, "more controlled review of 102 additional images to pressure-test our findings". It tested two large-scale AI vision models that are both freely available.

Gemma3 27B (built by Google DeepMind) correctly identified the city and country of a travel photo 87 per cent of the time. Qwen3 VL 30B (developed by Alibaba's Qwen team) performed even better, reaching 91 per cent accuracy.

"Traditionally, phishing has been about casting a wide net: send the same

message to thousands or millions of people and hope a small percentage responds. AI makes it much easier to person-

AI & You



company McAfee, has tried to make sense of how much location information resides within an ordinary travel photo. The answer may astound you — some AI models can detect the location 90 per cent of the time. More important, this accuracy rate is achievable with tools that are free and widely accessible.

"AI isn't necessarily looking for one hidden clue. It's connecting lots of different details. That could be the architectural style, the vegetation, the shape of a mountain range or even something on a restaurant menu. None of those clues is especially revealing on its own but when AI connects all of them, it can be enough to identify where a photo was taken," Steve Grobman, chief technology officer, McAfee, tells **The Telegraph**.

Turning off location tagging or removing metadata before sharing a photo remains a good privacy practice. But AI can now analyse the image itself.

"An ordinary street scene in Mumbai or a beach photo from Goa can contain clues that AI can piece together to

alise those attacks. Instead of a generic phishing email, you might get a message that appears to come from your hotel saying that there's an issue with your reservation or asking you to verify a payment," says Grobman.

With geo-location inference this accurate, scammers do not need to cast a wide net. They can simply use publicly shared photos to build a believable context around an attack, such as "we detected unusual account activity while you were travelling in A", "your card was flagged for a transaction in B — please verify immediately", or "your reservation in C requires reconfirmation — click here to secure your booking."

Says Grobman, "The biggest thing to watch for is urgency. If a message tells you there's a problem with your booking, asks you to make a payment or pushes you to click a link right away, slow down and verify it. Go directly to the hotel, airline or travel company's official app or website rather than using the link or phone number in the message."