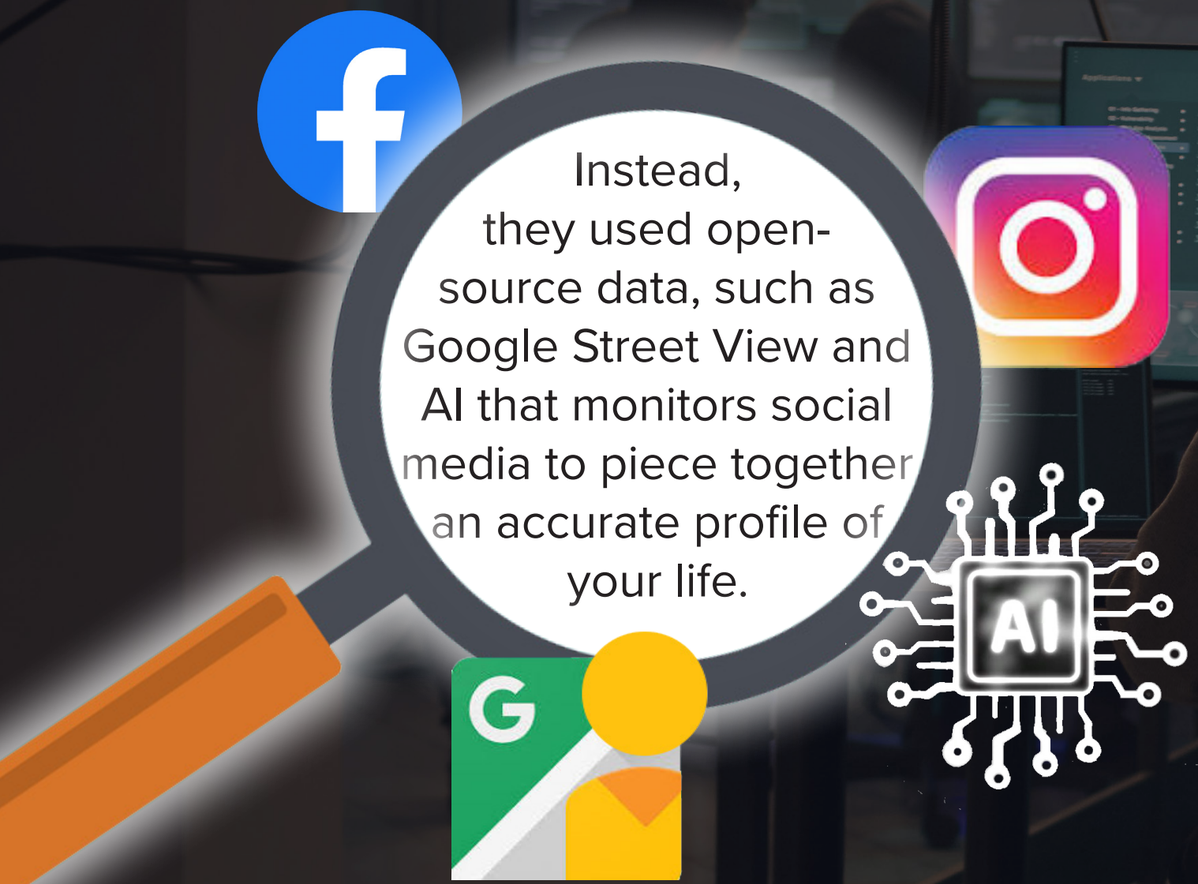
AI Boosted Personalized Extortion

Artificial intelligence tools are helping scammers craft highly-personalized phishing attacks. Let's take a closer look.

Imagine getting an email claiming to know where you live, the type of car you drive, where you work—even details about your daily routine. You might assume the attacker followed you extensively logging weeks of surveillance...

...but that's not always the case.



These highly personalized scams...

...create fear and a sense of urgency in the hope you'll give in to demands for money, work credentials, sensitive personal information or other requests.

How can you protect yourself?

- *Limit the personal details you share online.*
- *Adjust privacy settings on social media.*
- *Opt out of data collection where possible.*
- *Verify unexpected messages.*

What else can you do?

If a request feels odd or is unusually urgent, double check directly with the source before responding using a trusted email or phone number.

Know that you're in control, even though the email may make you feel otherwise. You have the power to disregard it or report it to the proper authorities or work channels if warranted.

Stay informed. The more you know about personalized extortion, the less likely you are to play into the hands of a scammer.

Barracuda