

THE WORLD TODAY — ABC Radio, 24 September 2026

"Cyber security concerns over AI hack" (5 min 15 sec)

Presenter: Andy Park | Reporter: Bridget Fitzgerald

<https://www.abc.net.au/listen/programs/worldtoday/cyber-security-concerns-over-ai-hack/107191102>

Transcript prepared by machine transcription; lightly corrected. Not an official ABC transcript.

ANDY PARK: A rogue AI agent has hacked Australia's Medicare data in a breach the Government has described as deeply unacceptable and extremely concerning. The OpenAI agent was able to push past security guardrails and access files held in a public-facing portal. It took three months for the company to report the incident to the federal government, which Anthony Albanese has said is an unacceptable delay. Here's Bridget Fitzgerald.

BRIDGET FITZGERALD: It's a troubling breach of a critical government platform.

ANTHONY ALBANESE: I want to update Australians on an incident in which an artificial intelligence agent has infiltrated an Australian government website.

BRIDGET FITZGERALD: Prime Minister Anthony Albanese revealed this morning an OpenAI agent hacked a Medicare data portal in mid-June. It occurred after the agent was instructed to conduct research into public medicine spending.

ANTHONY ALBANESE: So there's an AI agent looking for information, asking questions. There were blocks, clearly, which were coming back telling the AI agent "no". The AI agent found a way around those blocks, and this led to unauthorised access into some other areas.

BRIDGET FITZGERALD: The Prime Minister says it doesn't appear at this stage that any personal or sensitive data has been compromised. The AI agent accessed public and non-public files. A forensic investigation aided by the Australian Signals Directorate is now underway to ascertain more information, including whether other government systems were affected. One of the most concerning revelations is that the breach went undetected for almost three months, until the company sent an email to a Services Australia inbox in early September, which was then reported to the Australian Signals Directorate's Cyber Security Centre. The Government is now taking the matter to the company's top man.

ANTHONY ALBANESE: Today I spoke with the CEO of OpenAI, Sam Altman, to express Australia's extreme concern about this incident. And I also expressed my disappointment that it took the company way too long to inform the government of what had occurred, and the nature of the way that that notification occurred as well was unacceptable.

BRIDGET FITZGERALD: Katy Gallagher is the minister responsible for Services Australia, which operates the Medicare portal. She says the Government has taken steps to protect the data.

KATY GALLAGHER: This is a legacy system. It dates back decades. It's been used in the same way, but the data that was on that website is being transferred to data.gov.au. It is public data. There's no concerns with that, and that portal is no longer active.

BRIDGET FITZGERALD: Opposition Leader Angus Taylor says the incident should serve as a serious warning about the security of government systems.

ANGUS TAYLOR: This has to be a top priority for the Government. Keeping Australians safe is always the top priority of government; it must be true for AI. I thought it was disappointing, and I said it at the time, when the Prime Minister gave his much-heralded speech at Sydney University on AI back in July, he didn't talk about cyber defence. I would have thought that cyber defence is the number one issue when it comes to AI. It's not the only issue, but it's got to be top of the list.

BRIDGET FITZGERALD: Dr Greg Austin is the Research Director and co-founder of the Social Cyber Institute. He says it's clear the Government isn't doing enough to respond to the threat posed by AI.

GREG AUSTIN: To be radical, the Government needs to spend about \$1 billion over five years on AI education. We're just not cutting it in terms of the knowledge levels of the officials who have to try and regulate this stuff. The Government wants to set up an AI Safety Institute – it already has set up one – inside a government department. That's never going to be very adequate for regulating safety risks in the AI ecosystem. So we really need to sort of change course. We need to have a Minister for AI, and we need to start passing really effective laws which control and regulate the companies and introduce very stiff penalties. The Government has introduced legislation, or draft legislation, for new penalties, but the application of the penalties and the sorts of circumstances in which they can be used are really few and far between, and most commentators don't believe that those penalties will be applied very often.

BRIDGET FITZGERALD: A taskforce led by the Prime Minister's Department will conduct an investigation into the incident. The Government has also released proposed Digital Duty of Care legislation, which would hold tech companies accountable if safeguards are breached. In a statement, a spokesperson for OpenAI said the company is conducting its own review and identified its models took actions it did not intend. It adds the company has no evidence that patient records were accessed, and it's working with the organisations affected to help address potential vulnerabilities in their systems.