# Foreign adversaries use AI to create fake local news sites ahead of Australian elections



Most Australians encountering local news websites like The Birdsville Herald may assume they are authentic sources, but some of these sites are in fact created by foreign adversaries to blend genuine news with fabricated stories. This tactic involves naming such sites after regional towns, often appending terms like ‘Herald’ or ‘Times’, making them appear credible to unsuspecting readers. These deceptive platforms can quickly distribute false narratives through social media channels and sometimes find their way into mainstream news reporting.

Mark Anderson, National Security Officer for Microsoft Australia and New Zealand, explained that these so-called “pink slime sites” are used in foreign influence campaigns to mislead readers. “Foreign influence campaigns use deceptive sites, known as pink slime sites, that appear credible however seek to trick readers into sharing false narratives,” Anderson said. The rise of generative AI has made it easier and faster for threat actors to establish such sites, while AI-driven language translation further enhances their plausibility.

Such activity often escalates around election periods, with an increased number of these sites appearing as adversaries ramp up influence operations. Anderson pointed out that the 48 hours before and after an election are particularly vulnerable times for increased deceptive activity in Australia. “It’s also the 48 hours either side of the election when we are most likely to see an increase in activity, so Australians should remain vigilant during this period,” he noted.

Heading into the 2024 electoral cycle, concerns about AI being used to manipulate voters were significant on a global scale. Ginny Badanes, who leads Microsoft’s election protection efforts, observed that although AI-driven deception did not reach the feared scale, notable instances did occur. “We didn’t see this happen on the scale many feared, but there were still notable instances of AI-driven deception – some of which were incredibly difficult to detect,” she said.

Among the AI-driven tactics employed were voice, video, and image deepfakes, alongside a rise in scams exploiting election-related urgency. Badanes highlighted voice deepfakes as particularly convincing and difficult to detect, citing instances in last year’s elections where real people were made to appear as if they said things they did not. The Australian Broadcasting Corporation recently demonstrated this risk by creating an AI-generated voice recording of Senator Jacqui Lambie, produced with her consent, illustrating how realistic such fabrications can be.

In terms of visual manipulation, AI-edited images may be more about subtle alterations rather than fully generated fake images. “Tiny edits can completely change the meaning of the image and fuel the spread of false narratives,” said Badanes. Scams also tend to spike during elections, with criminals using calls, texts, or emails purporting to be urgent requests related to electoral roll updates or fines to trick recipients into clicking malicious links or divulging personal information. Anderson advised, “Australians should be aware of calls, texts or emails that ask them to urgently click a link to do things like update their electoral roll details or risk fines. These very well could be malicious links, and the best advice is always to pause, verify and go directly to official sources if you’re unsure.”

The surge in cyber threats and scams around major events such as elections or the Olympics is not unusual. Cybercriminals exploit heightened public interest during these periods to intensify phishing scams, disinformation campaigns, and manipulation attempts. Badanes observed a continuous stream of threat activity throughout election periods, with peaks at critical points. She explained that the motives behind such attacks vary—from creating confusion and chaos to influencing voter opinion, engaging in espionage, or pursuing financial gain through scams. Often these aims can overlap.

The spread of manipulated content becomes particularly swift during emotionally charged or competitive times, like the final 48 hours before an election. Foreign actors have demonstrated significant agility in injecting and rapidly disseminating deceptive material during these critical moments.

Badanes emphasised the importance of cultivating critical thinking and scepticism among the public to combat these influence campaigns. “If something you see online fits a narrative too perfectly, it’s worth pausing to question if the source is credible or if the content could have been manipulated by AI or clever editing,” she commented. Developing this habit can reduce the effectiveness of deceptive content and slow misinformation and disinformation spread.

She drew parallels to well-known scams of the past, such as the “Nigerian prince” email frauds, noting that most people no longer fall for them because they have learned to question suspicious communications. “We don’t need to distrust everything – just make sure we’re verifying information sources,” Badanes concluded.

The Microsoft report illustrates a complex and evolving threat environment where AI technology is being harnessed to subvert electoral processes and public trust, particularly through the creation of fake news sites and sophisticated deepfake media, alongside scams targeting unsuspecting voters. It underscores the heightened risks associated with election cycles, especially within 48 hours on either side of the vote, offering insights into the nature and scope of these foreign influence campaigns and cybercriminal activities.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.aspi.org.au/report/hacking-democracies> - This report discusses how foreign adversaries create deceptive news sites, referred to as 'pink slime sites,' to spread disinformation and influence public opinion during election periods.
* <https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums> - This research highlights the use of cyber-enabled foreign interference in elections, including the creation of fake news sites and the spread of disinformation to undermine democratic processes.
* <https://www.cairnspost.com.au/news/breaking-news/prorussia-news-sites-spew-incendiary-us-election-falsehoods/news-story/5393899096558443c4c87ec694aff9e0> - This article reports on pro-Russia news sites spreading false information about the US election, illustrating how foreign influence campaigns use deceptive sites to disseminate false narratives.
* <https://www.opb.org/article/2024/11/12/foreign-influence-efforts-reached-a-fever-pitch-during-the-2024-elections/> - This article details how foreign influence efforts intensified during the 2024 elections, including the use of deceptive sites to spread false narratives.
* <https://www.klcc.org/npr-politics/2024-11-09/foreign-influence-efforts-reached-a-fever-pitch-during-the-2024-elections> - This article discusses the surge in foreign influence efforts during the 2024 elections, including the spread of false information through deceptive news sites.
* <https://www.aspi.org.au/report/hacking-democracies> - This report examines how foreign adversaries use deceptive news sites, known as 'pink slime sites,' to spread disinformation and influence public opinion during election periods.
* <https://news.google.com/rss/articles/CBMitgFBVV95cUxQcU5mSkRmVWNtUjZkampGR3NxUTFpS1FrYzJzSEdEMHFQM2NrU21PLUJiMkdzVlQ1bGpDbTk3ak5PNlZUQnhEa1hZWklTNTFiMDN4YV82djlyZjY3bFFVODduOG94WEdraHpfQUt1amhjRUcwOVdUbkN3Z3FTM0x1WkUtdDY4Z1ZhSHk1TGxTX0pxVDYzc1dHVnIxRldTcUhWbkU2Q2dtRmpsc3JhZ0xndnpZekpuQQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data