

Yahoo email hack affected Australian politicians

THOUSANDS OF AUSTRALIAN government officials, including high-profile politicians and senior defence officials, are among the one billion victims of a massive Yahoo data breach, according to information obtained by the ABC.

Data provided by US security company InfoArmor, which alerted Australia's Department of Defence last October to the massive data breach, reveal more than 3000 log-in credentials for private Yahoo services were linked to Australian government email accounts.

InfoArmor, an Arizona-based cyber security firm that investigates data theft for law enforcement agencies, said the data was stolen from Yahoo in 2013 by a hacker organisation from Eastern Europe.

It said the hacker group then sold the Yahoo accounts to cyber criminals and a suspected foreign intelligence agency for \$US300,000 each.

Yahoo revealed late last year it believed hackers stole data from more than one billion user accounts in August 2013, in what is thought to be the largest data breach at an email provider.

The stolen database contains email addresses, passwords, recovery accounts

and other personal identifying data belonging to a startling array of senior Australian officials.

Among those affected were Social Services Minister Christian Porter, Shadow Treasurer Chris Bowen, Victorian Premier Daniel Andrews, Liberal MP Andrew Hastie, opposition health spokesperson Catherine King and Liberal senator Cory Bernardi.

It is unclear how many of the accounts are still active.

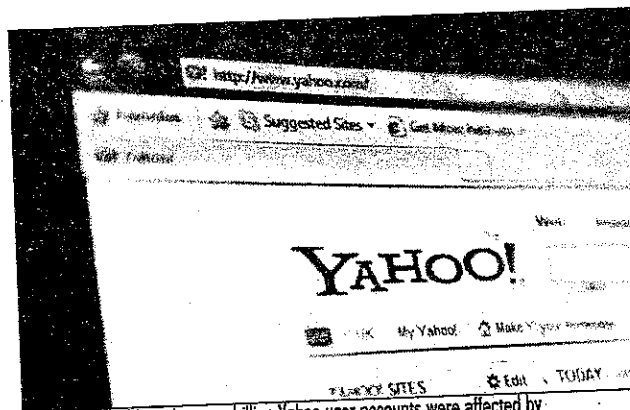
Australian Prime Minister Malcolm Turnbull said he would be getting a report from his cybersecurity advisor.

"It would be very unlikely that - referring to the politicians involved that I've seen - that there would be security issues, but we don't take any of this stuff lightly."

The ABC identified officials in the dataset because they used their government emails as back-ups if they forgot their passwords.

Last week, the ABC approached each of these affected politicians' offices, as well as some public servants, seeking confirmation of the authenticity of these log-in credentials. Most declined to do so.

The compromised accounts



More than one billion Yahoo user accounts were affected by the email hack in August 2013. Photo: 123RF

do not exclusively relate to clients of Yahoo's email service, but also Yahoo-affiliated web services such as the microblogging site Tumblr and the photo sharing site Flickr.

A spokeswoman for Mr Porter said "as far as the minister is aware he has never used a Flickr account".

A spokesperson for Senator Bernardi said "to the best of his knowledge, [Senator Bernardi] doesn't have a Yahoo account".

One advisor told the ABC it was possible some accounts linked to politicians were set up by former staffers.

Others who did respond confirmed the log-in credentials were accurate.

Accounts linked to police, judges

compromised

Other government officials compromised include those carrying out sensitive roles such as high-ranking Australian Federal Police officers, AusTrac money laundering analysts, judges and magistrates, political advisors and even an employee of the Australian Privacy Commissioner.

Alastair MacGibbon, the Prime Minister's Cyber Security Special Advisor, described the size of the Yahoo breach as breathtaking.

"It's really what's inside those accounts that matters," Mr MacGibbon added.

"If there are compromising activities inside those accounts - again, whether I work for a corporate or government it doesn't really matter - criminals

may exploit that. Criminals may exploit me recycling a password."

Mr MacGibbon said the magnitude of the breach made it hard to determine precisely how many of the affected Australian accounts were currently active.

The ABC understands the Yahoo account belonging to Mr Andrews has not been used by him in years.

The revelations come shortly after a Gmail account belonging to Hillary Clinton's campaign chairman, John Podesta, was compromised and its contents leaked at a critical juncture during the US election.

Some Democrats say the Podesta email leaks contributed to Mrs Clinton's loss by exposing years of his private communication to the world.

The Podesta saga demonstrated just how damaging a single compromised private email account could be.

— Risk email details could be used against victims

Professor Richard Buckland from the Australian Centre for Cyber Security said there could be serious embarrassment awaiting Australian officials from this Yahoo breach.

"There's potentially information in there that is blackmail-able," he said.

"Perhaps records of transactions of purchases, or discussions or things they've done. Private conversations that they didn't want to do on a government server. Perhaps they've engaged in some sort of shady activity. Or just expenses for politicians, for example, that they might have tried to keep out of official channels.

"Blackmail information is very valuable to other governments for nudging or persuading people to do things."

Another challenge facing the government is how to deal with compromised private accounts belonging to some Australian diplomats and special defence personnel posted overseas. Many of the officials featured in the dataset are employed in roles with security clearances that are intended to be low-profile.

"If I was in a position where my relationship with the government wasn't to be known by others, then absolutely you shouldn't be linking a government account to your personal accounts," Mr MacGibbon said.

—Reuters