+NEWS |

‘Fake app’ attack targets Green Cross Health practices

Stephen Forbes
sforbes@nzdoctor.co.nz

Thursday 4 July 2024, 03:56 PM

1

3 minutes to Read

A spokesperson for the National Cyber Security Centre says the health sector is a lucrative target for cybercriminals [Image: dem10 on iStock]

Green Cross Health's The Doctors chain of general practices has been the target of a fake app cyberattack.

The incident was outlined in a newsletter to staff last week.

Green Cross Health national operations manager Andrew Tucker says it was first alerted to the online scam by a patient on 19 June.

"One of our patients brought it to our attention after finding it when they searched Google for The Doctors app," Mr Tucker says.

Staff acted quickly after being notified and informed the National Cyber Security Centre NZ to have it blacklisted and also reported it to Google to get it removed.

"We also informed patients across all Green Cross Health practices who use The Doctors app," he says.

READ MORE

- **NEWS: Te Whatu Ora warns of email phishing scam**
- **NEWS: Te Whatu Ora grapples with secure data access for non-registered health workers**
- **NEWS: Lessons learnt from PHO hack attack: Financial struggles add to challenge of cyber vigilance**
- **NEWS: Investigation under way into cyber attack targeting thousands of coronial and health files**

Staying vigilant for scams

The message to patients is to remain vigilant of scams and only use the official The Doctors website, or the Google Play Store or Apple Store to download it directly, Mr Tucker says.

“This is the first time Green Cross Health medical division have been a target of this type of cyber-attack of a fake app posing as an official one.”

But it is a common phishing scheme for online scammers trying to gain access to people’s information.

Maintaining the security of its patient data is vital, Mr Tucker says.

“We want to let our patients know that if they already have The Doctors app, their data is safe and secure.”

Cyber security experts respond

In an emailed response to questions from *New Zealand Doctor Rata Aotearoa* a spokesperson for the National Cyber Security Centre says the health sector is a lucrative target for cybercriminals as there's a large amount of personal and sensitive information.

"Part of the advice we give organisations like this, is that education of staff is as important as technical measures when it comes to stopping cyber incidents. Fake apps are not a common type of cybercrime, we might see two or three incidents a year, but they do happen.

"If you're concerned that you may have downloaded a fake app or may have given over information, contact CERT NZ and we can give you advice on the next steps to take."

Te Whatu Ora aware of incident

In an emailed response to questions, Te Whatu Ora chief information and security officer Sonny Taite says it is aware of the incident involving Green Cross Health. The fact Green Cross Health reported it to the National Cyber Security Centre is the right step to take to enable it to receive the support it needs, Mr Taite says.

“Phishing and social engineering scams are a constant threat for all organisations, and we advise all of our health partners to stay vigilant for scammers, particularly if being asked to provide information.”

Warning to health providers last month

Just last month, Te Whatu Ora warned health providers to be on the lookout for suspicious messages after it identified an email phishing scam targeting health organisations.

Mr Taite outlined the cyber security threat during a presentation to an online stakeholder hui by the agency on 12 June. The emails tended to look like file-sharing requests and appear to be legitimate.

Recent cyberattacks in the UK, which had crippled London NHS hospitals and general practices, were highlighted by Mr Taite. Several hospitals declared the attacks as critical incidents, cancelling operations and tests, and emergency department patients had to be diverted.

Meanwhile, on 6 June, the Australian Information Commissioner filed a lawsuit against one of Australia's largest private health insurance providers, Medibank, for failing to take reasonable steps to protect patient data from misuse.

The company was the victim of a ransomware attack in October 2022, involving patient data of 9.7 million people. The company refused to pay the ransom and, in November 2022, the Russian hackers released the data on the dark web.

TELL US WHAT YOU THINK

You can add your comments using the comment function below, or by sending a Letter to the Editor to **editor@nzdoctor.co.nz**