+NEWS |

Te Whatu Ora warns of email phishing scam

Stephen Forbes

sforbes@nzdoctor.co.nz

0

Wednesday 12 June 2024, 04:42 PM

3 minutes to Read

Cyberattacks last week crippled London NHS hospitals and general practices [Image: Gorodenkoff on iStock]

> “This is an indication that we’re not siloes in healthcare, and we are all connected”

Health providers are being warned to look out for suspicious messages after Te Whatu Ora identified an email phishing scam targeting health organisations.

The agency’s chief information and security officer, Sonny Taite, outlined the latest cyber security threat during a presentation to an online Te Whatu Ora stakeholder hui today. Mr Taite says the emails tend to look like file-sharing requests and appear to be legitimate.

“Please be on high alert. PHOs are working to bring awareness to you all. As per usual, we are constantly under attack,” he told the hui.

READ MORE

- **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**
- **NEWS: How secure is your practice from cyberattack?**

As an example, Mr Taite highlighted cyberattacks last week, which crippled London NHS hospitals and general practices. Several hospitals declared the attacks 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.

Te Whatu Ora on alert

“That is one example we don’t want to see here,” Mr Taite says. “It can be very destructive to an organisation, so it’s critical to maintain our cybersecurity.”

He says the Medibank case in Australia and the NHS breach in the UK highlight the risks associated with cyberattacks.

“This is an indication that we’re not siloes in healthcare, and we are all connected.”

Some ransomware attacks can take over an entire network in as little as 45 minutes, meaning health providers must be vigilant, Mr Taite says.

“Everyone now relies on digital technology. But you need to know when you are securing services that they are safe.”

The first step is assessing an organisation’s risks. An organisation with an internet-facing system with a single factor of authentication is in greater danger of attack, he says.

Being prepared for a cyberattack

Mr Taite also outlined what can be done to counter cyberattacks during his presentation. In 2023, there were 30 billion password attacks a month globally, and vulnerable systems are constantly being targeted. Unmanaged internet gateway devices remain the most common method used by attackers to gain access. But he says cloud computing attacks are on the rise, increasing by 75 per cent year-on-year.

Security framework

Last year, Te Whatu Ora upgraded its health information security framework to better accommodate the different organisations that make up the country's health system, from small individual general practices that employ up to 25 people to hospitals and suppliers employing thousands.

The framework helps support all health sector organisations in managing and improving the security of their information and outlines the security requirements for different providers.

All organisations in the health sector should watch for any updates from Te Whatu Ora, Mr Taite says.

"Please keep checking our cyber hub regularly."

Te Whatu Ora chief executive Margie Apa echoes Mr Taite's thoughts.

"Cybersecurity is so important, not just to ensure we are protecting ourselves, but also the public. They trust us with their data and information, and we operate on the trust and confidence of our community," Ms Apa says. "It's really important as a collective that we pay specific attention to how we are protecting that information."

Global cybersecurity study

Research released by IT security company NordPass in September found cybersecurity is an issue for health systems worldwide.

The international study said health was among the top 10 industries for client data leaks. Since 2019, hackers have attacked nearly 300 health organisations worldwide.

A ransomware attack on the former Waikato DHB in May 2021 targeted hospital computer and phone systems to obtain information related to patients, staff and finances.

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**

You can view your CAPTURE RECORD here.