

KEEP YOUR PRACTICE SAFE.

Phone them and ask.

A phishing attack is targeting medical and allied health practices across Victoria.

The email comes from a real practice you know. Their account has been taken over. They do not know.

Antivirus does not stop it. Link scanners come back clean.

WARNING SIGNS

- It asks you to open the link on a "Desktop or Windows Laptop"
- It arrived at an odd hour
- You were not expecting a file from them

IF SOMEONE ALREADY CLICKED

- Say so straight away. Nobody is in trouble.
- Unplug that computer from the network.
- Call your IT provider.

Phone the sender and ask if they sent it. Thirty seconds.

Do not reply to the email — if they are hacked, the attacker answers.