Suspicious Email Incident

Dear Patient,

Thank you for contacting Cavendish Road Clinic regarding the suspicious email and link that you may have received. We understand that this situation may be concerning and appreciate your patience while we investigate the matter.

What You Should Know

The link identified in the email was associated with a ScreenConnect (ConnectWise Control) executable. A ScreenConnect session generally requires additional user actions before remote access can be established.

If You Only Clicked the Link

If you only clicked the link and did not download, install, or run any software, the risk is generally considered low. Simply opening a webpage does not normally establish a ScreenConnect remote support session.

Mobile Phone Users (iPhone and Android)

Patients who accessed the link from a mobile device can generally be reassured. In most cases, simply clicking a link on an iPhone or Android device does not establish a ScreenConnect session. Additional steps would typically be required, including downloading an application, installing it, granting permissions, and approving a connection.

If you used a mobile phone and only clicked the link, or downloaded a file but did not install any application or grant permissions, the risk is generally considered low.

As a precaution, please check whether the ConnectWise Control or ScreenConnect application has been installed on your device. If it is not installed, and no permissions were granted, there is generally a much lower risk of remote access occurring.

If You Downloaded, Opened, or Ran the File

If you downloaded, opened, or executed the file from the email, additional precautions are recommended. ScreenConnect is remote access software and running the file may have allowed further actions to occur.

Immediate Actions

- Disconnect the device from the internet immediately by turning off Wi-Fi, disconnecting any network cables, and disabling mobile data where applicable.
- Do not use the device for sensitive activities such as internet banking, accessing email accounts containing sensitive information, or logging into government services until it has been assessed.
- Check whether ConnectWise Control or ScreenConnect is installed on the device.

- Check whether a ScreenConnect or ConnectWise-related folder exists on the device. Windows users should check Program Files, Program Files (x86), ProgramData, and AppData folders.
- Check whether ScreenConnect or ConnectWise Control is present and running as a Windows service.

If ScreenConnect Is Installed, Running, or a Folder Exists

- Disconnect the device from the internet immediately if you have not already done so.
- Do not continue investigating the device unless you have appropriate technical expertise.
- Reset passwords straightaway, use a different device to reset passwords if possible.
- Speak with a qualified IT professional immediately.
- The IT professional should assess whether a remote access session was established, whether any unauthorised activity occurred, whether additional malware is present or further remediation are required.
- Run a full antivirus or endpoint security scan using up-to-date security software.
- Review installed applications and remove any software identified by your IT professional as suspicious.
- Install all available operating system and security updates.
- Change passwords for important accounts if you entered credentials after clicking the link.
- Enable Multi-Factor Authentication (MFA) wherever possible.
- Monitor email, banking, and other important accounts for unusual activity.

When to Seek Immediate Assistance

- You ran the downloaded file.
- You installed ScreenConnect / ConnectWise Control.
- You approved connection requests or permissions.
- You find ScreenConnect installed, running, or present on the device.
- You observe unusual device behaviour or believe someone may have remotely accessed your device.

Additional Support

For independent cyber security guidance, patients may contact the Australian Cyber Security Hotline on 1300 292 371 or visit www.cyber.gov.au.

Important Notice

Cavendish Road Clinic cannot determine whether any individual patient device has been affected. This advice is general guidance only and is intended to help patients assess their level of risk and undertake appropriate precautions.

Our Apology

We sincerely apologise for the delay in responding and for any concern this incident may have caused. We appreciate your understanding while we work through a high volume of enquiries.

We also appreciate that patients may be frustrated by the time taken to provide a response. The clinic has been obtaining technical advice and cybersecurity guidance to ensure that the information provided to patients is accurate and appropriate to the circumstances. Our priority has been to provide reliable information that is specific to this incident, and we thank patients for their patience and understanding while this work was undertaken.

Kind regards,

Cavendish Road Clinic