



Security Issue Identified in PHP

Dear Club Presidents and Secretaries,

A serious security issue has been identified in **PHP**, software that runs behind many websites, including WordPress. If an affected website isn't updated, an attacker could take control of it, change its content, or access information stored on the website.

Please contact whoever looks after your club's website today. This may be your website developer, hosting company, managed IT service provider (MSP), or a technically minded club member. You do not need technical knowledge to take the steps below.

This alert does not mean your club has been hacked. However, a website can look and work normally while still being vulnerable.

1. Forward this email to your website provider

Ask them to urgently check whether your club's website, and any other websites or online services they manage for the club, are affected. You can copy and paste this request:

Please urgently check our website for the PHP security vulnerabilities CVE-2026-109618 and CVE-2026-109619, also known as "PHP2Shell".

Please confirm whether we are affected and, if so, install the required PHP security updates as a priority. Please check the PHP software running on the hosting server, not just WordPress, plugins, or themes.

Please ensure we have a current backup, test the website after updating, and check for signs of unauthorised access or changes. If you cannot apply the updates promptly, please advise what immediate protection is possible and whether the affected service needs to be temporarily taken offline.

Please provide written confirmation of the outcome, including any outstanding work and when it will be completed.

2. Follow up until you receive a clear answer

Ask your provider to confirm that your website is either **not affected** or **has been updated to address both vulnerabilities**. If work is still outstanding, obtain a completion time and follow up.

Updating WordPress or its plugins alone may not fix this issue. Your provider also needs to check the underlying PHP software.

3. Escalate if you cannot get help

If you don't know who manages your website, cannot reach them, or they cannot confirm what action is needed, contact the [SLSNSW ICT Team](#) with your club name and website address so we can help identify the next step.

If your provider identifies signs of a possible breach, please follow your data breach protocols. Ask the provider to preserve relevant records and investigate, as installing the update alone will not undo an earlier compromise. If you need help, please contact the [SLSNSW ICT Team](#).

4. Confirm who will maintain your website going forward

Once this issue is resolved, confirm who will maintain ongoing security updates and backups, including the hosting software. Someone who updates website content does not necessarily maintain its security.

Technical guidance for your provider is available in the [official PHP security advisory](#).

Thank you for acting promptly to help protect your club, its members and visitors to your website.