



Yorkshire Cricket Southern Premier League

www.ycspl.co.uk

Beware of Scams

We have recently had reports of scam emails being sent to members that appear to come from League officials. Unfortunately, criminals use a technique called email spoofing, which makes it look as though the email genuinely came from a trusted address — even when it hasn't.

What is email spoofing?

- Just like anyone could write your name and return address on an envelope, criminals can fake the 'from' field in an email. This doesn't mean the account has been hacked — it's simply a way to make scams more believable.

What you need to know

- Emails may look like they've come from a real YCSPL address, even if they haven't.
- Don't rely on the sender's name or email address alone — spoofed emails can show the exact real address.
- Official League emails will normally include a proper YCSPL signature and logo (unless sent from a mobile in a reply).

How to protect yourself

- Be suspicious of emails asking for unusual actions — such as transferring money, buying vouchers, or sharing personal details.
- If something doesn't feel right, stop and verify:
 - call the person on a known phone number *or*
 - start a fresh email (don't reply to the suspicious one).
- Never click links or open attachments in an email you're unsure about.
- When in doubt, delete the message or double-check with the sender first.

Final word

Scam emails are, sadly, part of modern life. By staying alert, verifying unexpected requests, and not rushing into action, you can avoid falling victim.

Don't Trust at Face Value

- the "From" address can be faked
- emails may look like they come from a real address

Do's

- check the message carefully – does it look unusual?
- verify requests by phoning or sending a fresh email
- delete it if you're not sure

Don'ts

- don't transfer money, buy vouchers, or share personal info by email
- don't click links or open attachments you weren't expecting
- don't reply directly to suspicious emails

Stay alert. If in doubt — check first, act later.

For more detailed guidance on spotting scams in general, please look at the [National Cyber Security Centre website](#)