

Renew Safely: Stay One Step Ahead of Spam Emails

As the annual registration renewal period gets under way, the General Chiropractic Council (GCC) is reminding registrants to remain alert to fraudulent or misleading emails.

Why you are seeing this

The GCC has received a report of a suspicious email claiming to represent the Council but originating from a non-GCC email domain. We are reviewing the matter. The receipt of a suspicious email does not, by itself, establish that GCC systems or personal data have been compromised.

Fraudsters may use an organisation's name, branding or publicly available information to make their communications appear genuine. An email may also create urgency by asking you to renew your registration, make a payment or provide personal information quickly.

1 Pause

2 Check

3 Report

1

STEP 1

Pause

Do not rush to reply, pay or provide personal information.

2

STEP 2

Check

Check whether an email is genuine

Before responding or taking any action:

- Check the sender's complete email address, not just the displayed name.
- Look carefully for subtle misspellings or lookalike domains, including additional letters, substituted characters or different endings, such as .com instead of .org.
- Official GCC emails will normally come from an address ending in **@gcc-uk.org**.
- Where an authorised service provider contacts you on our behalf, the relationship and purpose of the communication should be made clear.
- On a computer, hover your cursor over a link without clicking it to view its actual destination. If the address is unfamiliar, unclear or different from the expected GCC address, do not click it.
- On a mobile device, the safest approach is to access the GCC website or registration portal directly rather than following an unexpected link.
- For anything related to your CPD or registration retention, always log in to the GCC Registrant Portal directly, either by visiting the official GCC website at www.gcc-uk.org and clicking "Chiropractor Login" at the top of the page, or by going to <https://gccportal.imiscloud.com>. Please avoid using links in unexpected emails.
- Be cautious of unexpected attachments, urgent payment demands or requests for personal or financial information.
- GCC will never ask you to disclose your password, security codes or multi-factor authentication codes.
- If you are uncertain, contact GCC using the details published on our official website (<https://www.gcc-uk.org>) rather than those contained in the email.

**STEP 2 CONTINUED**

The GCC's official email domain is protected by enforced and actively monitored DMARC controls. These controls help prevent criminals from spoofing our exact domain. However, they cannot prevent someone from registering and using a similar-looking domain, so it remains important to check the full sender address carefully.

3**STEP 3****Report****What to do if you receive a suspicious email**

If an email claims to represent the GCC but appears suspicious:

1. Do not click any links, open attachments, reply or make a payment.
2. Retain the original email, as it may assist our investigation.
3. Forward the email as an attachment to dpo@gcc-uk.org.
4. You can also forward suspicious emails to the National Cyber Security Centre at report@phishing.gov.uk or use the NCSC phishing reporting service (<https://www.ncsc.gov.uk/collection/phishing-scams>). When reporting an email to GCC, please do not include passwords, security codes, banking credentials or unnecessary personal information.

**If you have already responded**

If you have clicked a link, opened an attachment or provided information:

- Contact GCC immediately using the details on our official website.
- Change any password you disclosed, using the genuine website or application.
- Change the password on any other account where you used the same password.
- Contact your bank immediately if you provided payment details or made a payment.
- Monitor your accounts for unusual activity.

**How we will use information you provide**

GCC will use information submitted through a phishing report to investigate the communication, protect registrants and help prevent fraud or unauthorised access.

Information will be handled securely, shared only where necessary and lawful, and managed in accordance with our privacy notice (<https://www.gcc-uk.org/privacy-policy>).

Your vigilance helps us protect registrants and maintain the security and integrity of the registration process.