7 STEPS TO DETECT PHISHING SCHEMES

1 Feels Off?

Trust your gut. If the email doesn't feel right, **don't even open the message**. Start investigating from your inbox.

2 Check the Name

Ensure the sender's email address is coming from @**dcpglobal.com**. Dangerous people use extensions like **.co, .org, .info**.

3 Hover, Don't Click

When you hover over the hyperlinked email or website, verify that it matches what the text says.

4 Request for Money

If you are asked to pay to gain access or apply for a job, **do not respond**. This is a phishing scheme!

5 Typos

Look carefully for typos in the text that could reveal that the message was not written by a professional in the industry.

6 Too Good to Be True

If the email is promising you something unrealistic pay for little to no work, it's likely a red flag. Exercise caution!

7 Still Unsure? Contact Us Directly.

jobs@dcpglobal.com

DCP

dcpglobal.com